Marquette Law Review

Volume 106
Issue 1 *Fall*

Article 5

Fall 9-1-2022

Legal Implications of a Ubiquitous Metaverse and a Web3 Future

Jon M. Garon

LEGAL IMPLICATIONS OF A UBIQUITOUS METAVERSE AND A WEB3 FUTURE

JON M. GARON*

> The future influences the present just as much as the past.
>
> **—Friedrich Nietzsche**[1]

> [T]he present agony of social isolation, the impersonality, structurelessness, and sense of meaninglessness from which so many people suffer are symptoms of the breakdown of the past rather than intimations of the future.
>
> **—Alvin Toffler**[2]

The metaverse is understood to be an immersive virtual world serving as the locus for all forms of work, education, and entertainment experiences. Depicted in books, movies, and games, the metaverse has the potential not just to supplement real-world experiences but to substantially supplant them. This Article explores the rapid emergence and evolution of the Web3 technologies at the heart of the metaverse movement. Web3 itself is a paradigmatic shift in internet commerce.

This Article begins by exploring the competing economic and philosophical approaches to the future of the internet, which is being driven on one hand by the most successful internet advertising firms (Facebook and Google) as well as their video game competitors (Roblox, Microsoft's Minecraft, Epic Games, and Valve) and on the other hand by Web3 advocates focusing on cryptocurrencies, nonfungible tokens, decentralized finance (DeFi) and distributed autonomous organizations (DAOs). Limiting the focus on U.S. law, this Article reviews three core areas for the development of the metaverse: the

---

* Professor of Law, Nova Southeastern University Shepard Broad College of Law. The initial version of this paper was developed and presented at the American Bar Association Business Law Section Cyberspace Winter Working Meeting. Special thanks to Cheryl Butzl, Ed Morse, the members of the 2022 Winter Working Meeting, and Dan Garon. Available at SSRN: https://ssrn.com/abstract=4002551 [https://perma.cc/UYT9-VWRL].

1. *See generally* FRIEDRICH NIETZSCHE, HUMAN, ALL-TOO-HUMAN: A BOOK FOR FREE SPIRITS 18 (Helen Zimmern & Paul V. Cohn trans., Prometheus Books 2009) (1878) (the oft-quoted statement is not attributable to a publisher work) ("Our destiny rules over us, even when we are not yet aware of it; it is the future that makes laws for our to-day.").

2. ALVIN TOFFLER, THE THIRD WAVE 395 (1980).

regulatory environment; the transactional essentials; and the limits on governmental intrusion into the metaverse.

The review of the regulatory environment includes state and federal gambling laws, money transfer laws, securities laws, and regulation of unfair and deceptive trade practices used to enforce privacy and cybersecurity obligations. The section on transactional essentials focuses on contracts between metaverse enterprises and their customers, antitrust and competition restraints, copyright protections, protections of biometric data and rights of publicity, and protections of customer speech in metaverse environments. Finally, this Article addresses the need for the continuing evolution of the Fourth Amendment protection from search and seizures, the third-party doctrine limitations on reasonable expectations of privacy, and the statutory protections under the Stored Communications Act.

This Article highlights that although these doctrinal issues are not new, the scope of the metaverse and its potential social importance will reshape these doctrines in sometimes unpredictable ways. Technologists, practitioners, and regulators must be open to these shifts to appropriately develop the correct mix of user control, industry practice, and regulatory oversight.

I. INTRODUCTION

The metaverse, as highlighted by the recent corporate name change of Facebook to Meta Platforms, Inc. (Meta), owes its literary origins to Neal Stephenson's *Snow Crash* (1992) or to prior works by Verner Vinge and William Gibson.[3] The metaverse has been used in an informal manner for the past three decades. Aspects of a metaverse are essential to world-building games like *Roblox*, *Minecraft*, *Horizon's World*, and *Fortnite*, to massive multiplayer online roleplaying games like *RuneScape*, *Final Fantasy*, and *World of Warcraft*, and to virtual worlds like *Second Life*.[4] These online environments allow users to interact with each other, to engage with computer generated characters, and to play or perform activities using elements within the virtual environment. To foster the interaction among participants, each participant is represented by an avatar. The avatars may be designed to resemble the real-world user, to be highly fanciful, or to be anything in-between. As these examples suggest, there are already metaverses available for the public, and "the metaverse" actually reflects a multiverse composed of different metaverses. The term metaverse is generally used to cover the multitude of metaverses.

Although the metaverse remains in its nascent state, it will build on the current Web 2.0 internet. Matthew Ball has offered seven attributes that describe the metaverse as well as the current internet: persistence; synchronous and live interactions; the capacity for as many concurrent users as the users demand; a stable, functioning economy; the incorporation of both digital and physical worlds as well as operating on both open and closed platforms; being

3. *See* Ethan Zuckerman, *Hey, Facebook, I Made a Metaverse 27 Years Ago*, THE ATLANTIC (Oct. 29, 2021), https://www.theatlantic.com/technology/archive/2021/10/facebook-metaverse-was-always-terrible/620546/ [https://perma.cc/PV5Z-9STQ] ("[Stephenson's] vision of the metaverse owed a debt to Vernor Vinge's 1981 *True Names* and to a series of William Gibson novels from the '80s. Both of those authors owed a debt to Morton Heilig's 1962 Sensorama machine, and on and on we go, back in time to Plato's shadows on a cave wall.").

4. *See* Jon M. Garon, *Playing in the Virtual Arena: Avatars, Publicity, and Identity Reconceptualized Through Virtual Worlds and Computer Games*, 11 CHAP. L. REV. 465, 468–70 (2008).

largely interoperable; and being "populated by 'content' and 'experiences' created and operated by an incredibly wide range of contributors."[5]

One of the most important influences on the metaverse is the generation of users ready for it. The beginning of the 2021 drumbeat for the metaverse began with the public offering by *Roblox*, signaling to a generation raised in a virtual world rather than on a *Sesame Street* that their time had arrived.[6] As a result, a generation of young adults have grown up using the fifteen-year-old site for social experiences. It has hosted birthday parties,[7] concerts, an egg hunt, a tie-in with Gucci to celebrate the latter's 100th anniversary, and an agreement with Nike.[8] In addition, Snapchat's 3D Bitmoji function launched in July 2021, allowing its 280 million daily active users to create avatars for augmented reality.[9] The Bitmoji integration provides a powerful shift in user experience.

---

5. Matthew Ball, *The Metaverse: What it is, Where to Find it, and Who Will Build it*, MATTHEWBALL.VC (Jan. 13, 2020), https://www.matthewball.vc/all/themetaverse [https://perma.cc/6P53-44AY]; *see* Ben Thompson, *Microsoft and the Metaverse*, STRATECHERY (Nov. 9, 2021), https://stratechery.com/2021/microsoft-and-the-metaverse/ [https://perma.cc/SQ6H-LJ96] (quoting Ball and noting that these attributes describe the internet as well).

6. Dean Takahashi, *The DeanBeat: Roblox Public Offering is a Vote about the Metaverse*, GAMESBEAT (Mar. 5, 2021), https://venturebeat.com/2021/03/05/the-deanbeat-roblox-public-offering-is-a-vote-about-the-metaverse/ [https://perma.cc/5V2D-L3SF]. ("Roblox, the platform for user-generated games, will go public through a direct listing of its shares on March 10. I see its pending success or failure as a stock as a kind of referendum on the metaverse . . . ."); Patrick Seitz, *Roblox Stock Continues Meteoric Rise on Metaverse Story*, INV.'S BUS. DAILY (Nov. 19, 2021), https://www.investors.com/news/technology/roblox-stock-continues-meteoric-rise-on-metaverse-story/ [https://perma.cc/CA5Z-SYJH] ("Roblox today provides a platform for playing video games and socializing in 3D virtual worlds. But Roblox stock is considered a play on the metaverse, a next-generation version of the internet."); ERIC SHERIDAN, MICHAEL NG, LANE CZURA, ALEXANDRA STEIGER, ALEX VEGLIANTE & KATHERINE CAMPAGNA, AMERICAS TECHNOLOGY: FRAMING THE FUTURE OF WEB 3.0, METAVERSE EDITION 4 (Goldman Sachs Equity Rsch. ed., 2021) ("Over the past 12 months, the term Metaverse began to gain traction shortly after Roblox's direct listing in March and more meaningfully saw higher levels of Google Search interest during the Q3 '21 earnings season as various management teams discussed elements of their business within the future Metaverse.").

7. *See* Peter Allen Clark, *The Metaverse Has Already Arrived. Here's What That Actually Means*, TIME (Nov. 15, 2021), https://time.com/6116826/what-is-the-metaverse/ [https://perma.cc/WH73-EFSZ] ("When Cathy Hackl's son wanted to throw a party for his 9th birthday, he didn't ask for favors for his friends or themed decorations. Instead, he asked if they could hold the celebration on *Roblox*.").

8. *See* Joe Dyton, *Will Facebook or Roblox be the Master of the Metaverse?*, CONNECTED REAL ESTATE MAG. (Dec. 9, 2021), https://connectedremag.com/das-in-building-wireless/wireless/will-facebook-or-roblox-be-master-of-the-metaverse/ [https://perma.cc/D759-LP7Y].

9. *See* Maria Lewczyk, *Snapchat Commits to the Metaverse With Launch of 3D Bitmojis*, VIRTUAL HUMANS (July 28, 2021), https://www.virtualhumans.org/article/snapchat-commits-to-the-metaverse-with-launch-of-3d-bitmojis [https://perma.cc/862Z-NERP] ("Snapchat also boasts an impressive amount of editing capabilities and augmented reality options for users, including a variety of filters and lenses to create content with, such as the latest viral hit allowing you to turn yourself into

"Snapchat users are three times more likely to experiment with augmented reality (such as filters, lenses, etc.) to try on products than those who do not use Snapchat."[10]

The shift by Facebook to adopt Meta as its name and embrace virtual worlds has received even more attention.[11] That attention alone is likely sufficient to spur additional companies to provide resources and innovations, making virtual worlds more significant in the video game, social media, and e-commerce sectors. As a result of this growth, there will be an increase in attention by all other industry sectors.

The metaverse of tomorrow may not look like the virtual environments described in *Ready Player One*, *Tron*, *Avatar*, or *The Matrix*, but it is likely to look much more robust than the original *Second Life*. Advances in technology and shifts in culture have the ability to create an environment that is different rather than merely a faster and better-rendered version of what has gone before. The expansion of 5G wireless connectivity and embedded "internet of things" products have the potential to make many household devices, vehicles, and machines become integrated into virtual worlds. Non-fungible tokens (NFTs) and other Web3 tools can also help stabilize and protect the value of in-world currencies and assets, an essential component of financial stability in a game or society.

Meta has had a slew of corporate acquisitions suggesting where it sees at least some of this growth, including "a deal to buy Within, the company co-founded by VR pioneer Chris Milk, best known for its Supernatural workout app[;] . . . Unit 2 Games, which makes a 'collaborative game creation platform' called Crayta; Bigbox VR, which makes a popular game for Facebook's Oculus VR goggles; and Downpour Interactive, another VR game-maker."[12] Facebook was extremely successful when it provided third-party application

---

a cartoon."); *see also* Tyler Lacoma & Paula Beaton, *What is Bitmoji? Everything You Need to Know*, DIGITAL TRENDS (Sept. 22, 2021), https://www.digitaltrends.com/mobile/what-is-bitmoji/ [https://perma.cc/L8YR-BPAR] ("Bitmoji is an accessory app for social media platforms that people use to create little cartoon versions of themselves, which they then use on their various social media accounts . . . . You create an avatar of yourself and create various comics, GIFs, expressions, and reactions that use this avatar.").

10. Lewczyk, *supra* note 9.

11. *See*, *e.g.*, *Introducing Meta: A Social Technology Company*, META: NEWSROOM (Oct. 28, 2021), https://about.fb.com/news/2021/10/facebook-company-is-now-meta/ [https://perma.cc/DE8F-55JB]; Kevin Roose, *The Metaverse Is Mark Zuckerberg's Escape Hatch*, N.Y. TIMES (Oct. 29, 2021), https://www.nytimes.com/2021/10/29/technology/meta-facebook-zuckerberg.html [https://perma.cc/RY97-GSZT]; Peter Kafka, *Facebook is Quietly Buying up the Metaverse*, VOX (Nov. 11, 2021), https://www.vox.com/recode/22776461/facebook-meta-metaverse-monopoly [https://perma.cc/P2H5-Z2LV].

12. Kafka, *supra* note 11.

programming interfaces to developers in its social media environment including Zynga, the publisher of *Farmville* and *Words with Friends*.[13] Much like Facebook's earlier success, the use of interactive gaming signals an aggressive expansion into the space controlled by Valve's Steam, Epic Games, Microsoft, and others.[14]

Improved goggles and the development of augmented reality glasses closer to that of the Microsoft HoloLens rather than the Oculus Quest will improve the user immersion.[15] Haptic sensors embedded in gloves, keyboards, and a growing list of devices and wearables will increase kinetic feedback. Increased computing power in cell phones along with chip availability may make one's cell phone into an always-on replacement for desktop and laptop computers. The expanding skill set of Siri, Google, and Alexa will create a different kind of computer assistant. Together, these technologies will make the virtual world as different from Pong as a laptop has evolved from an IBM Selectric typewriter.

To truly make the leap from a game or social experiment to the digital replacement for society's virus-infected meat space, a new generation of audiovisual input devices are needed to enable a person to switch from presenting as an avatar to providing a live camera view relatively seamlessly. Without cameras, a person's real-time nonverbal communication is lost.[16] It is

---

13. *See* Daniel Victor, *FarmVille Shuts Down, but Practices It Instilled in Users and Developers Live On*., N.Y. TIMES (Jan. 1, 2021), https://www.nytimes.com/2020/12/31/technology/ farmville-zynga-facebook.html [https://perma.cc/M2SH-UYYB] ("In early 2009, when Facebook was still nascent in its efforts to swallow as much of the internet as possible, online games were not yet the behemoth they would become. Then, that June, came FarmVille."); Chris Morris, *The Most Important Friendship: Facebook and Zynga*, CNBC (Sept. 13, 2013), https://www.cnbc.com/2012/05/15/the-most-important-friendship-facebook-and-zynga.html [https://perma.cc/R5RZ-W4XN] (" '[G]ames from Zynga have generated the majority of our payments and other fees revenue,' the company said. The rest of the revenue was tied to advertising. Zynga purchases a lot of ads on Facebook to promote its titles—and its apps generate a lot of page views . . . .").

14. Shani Shisha, *Fairness, Copyright, and Video Games: Hate the Game, Not the Player*, 31 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 694, 696 (2021) ("[V]ideo games now make up the largest entertainment market in the world by an order of magnitude.").

15. *See* Jamie Feltham, *HoloLens 2 Review: Ahead of Its Time, For Better And Worse*, UPLOAD (Apr. 9, 2021), https://uploadvr.com/hololens-2-review/ [https://perma.cc/6NPD-H95T] ("Unlike VR, which is—in its current form—mostly preoccupied with games and entertainment, HoloLens 2 shows you why AR has such remarkable potential for productivity and education. With the headset's new collaborative platform, Microsoft Mesh, I'm able to host meetings with other people that have genuine, tangible advantages over web calls, social VR platforms and physical meetings."); Will Greenwald, *Augmented Reality (AR) vs. Virtual Reality (VR): What's the Difference?*, PCMAG (Mar. 31, 2021), https://www.pcmag.com/news/augmented-reality-ar-vs-virtual-reality-vr-whats-the-difference [https://perma.cc/B5RV-FHYP].

16. *See* JUDEE K. BURGOON, VALERIE MANUSOV & LAURA K. GUERRERO, NONVERBAL COMMUNICATION 112 (2d ed. 2021).

already greatly diminished online, but a computer-generated avatar cannot replicate the eye movements, breathing, double takes, and tells that inform much of human communication.[17] Although there is some nonverbal communication through the proximity of avatars and manipulation of facial gestures, these are far less robust than face-to-face communications or communications through live video communications.[18]

If a combination of camera and augmented reality glasses were used instead of virtual reality (VR) goggles, however, the transition can be largely accomplished. Wearable haptic sensors could further enhance the nonverbal cues a person communicates to those on the other side of the conversations.[19] This is not the only possible solution. Cameras can also be used to map a user's live facial movement onto an avatar or digitally rendered image. Photorealistic avatars could create the illusion of being on camera when in fact, the person is wearing a VR headset that does not show inside the virtual world.[20]

Technological improvements such as those listed above are necessary but not sufficient for the creation of a fully realized metaverse. The other aspect of the change must come from social readiness, demand, and predisposition for

---

17. *See* Fatik Baran Mandal, *Nonverbal Communication in Humans*, 24 J. HUM. BEHAV. SOC. ENV'T, 417, 417–18 (2014) DOI: 10.1080/10911359.2013.831288 [https://perma.cc/56DQ-R4UT] ("Nonverbal behavior includes all communicative acts except speech. . . . It also includes bodily contact, posture, physical appearance, and direction of gaze and the paralinguistic variables of emotional tone, timing, and accent."); Patrick W. Miller, *Nonverbal Communication*, *in* NAT'L EDUC. ASS'N 10 (3d ed. 1988) ("Some facial expressions are readily visible, while others are so fleeting as to go unnoticed. Both types can positively or negatively reinforce the spoken word and convey cues concerning emotions and attitude. Next to words the human face is the primary source of information for determining an individual's internal feelings.") (citations omitted).

18. *Cf.* Masanori Takano & Takaaki Tsunoda, *Self-Disclosure of Bullying Experiences and Social Support in Avatar Communication: Analysis of Verbal and Nonverbal Communications*, 13 PROCS. OF THE THIRTEENTH INT'L AAAI CONF. ON WEB AND SOC. MEDIA 473, 474 (2019), https://ojs.aaai.org/index.php/ICWSM/article/download/3353/3221 [https://perma.cc/ZTK7-PPHA] ("Nonverbal communication is also important for self-disclosure and social support. Especially, avatar communication, where people with virtual bodies can show facial expressions and gestures in virtual space, allows us to nonverbally interact through the Internet. . . .") (citations omitted).

19. Earlier studies focused on the movement of avatars within virtual worlds. *See* Smiljana Antonijevic, *From Text to Gesture Online: A Microethnographic Analysis of Nonverbal Communication in the Second Life Virtual Environment*, 11 INFO. COMMC'N. & SOC'Y, 221, 225–27 (2008), https://doi.org/10.1080/13691180801937290 [https://perma.cc/W9GD-7K9Q].

20. *See*, *e.g.*, Adi Robertson, *Facebook Can Project Your Eyes Onto a VR Headset, and It's Exactly as Uncanny as it Sounds*, VERGE (Aug. 4, 2021), https://www.theverge.com/2021/8/4/22609564/facebook-reality-lab-reverse-passthrough-vr-prototype-research-siggraph [https://perma.cc/EMY4-YT3Q] ("Facebook Reality Labs . . . released a paper on 'reverse passthrough VR,' a recipe for making VR headsets less physically isolating . . . . 'Passthrough VR' refers to a feature that displays a live video feed from a headset's cameras, letting users see the real world while they're still wearing the device.").

use. Again, there are strong indicators that those changes are coming. The massive expansion of online gaming has led to a cultural shift among the millions who spend time in these environments, such as "(1) competitive integrity, (2) wealth sharing, and (3) labor."[21] Despite the overwhelming success of gaming, however, the metaverse will be built on more.

Expansion of at-home work accommodations and at-home educational environments makes use of Zoom, Slack, Teams, Canvas, and similar interactive environments a core part of one's work and learning environment. Separating work or school from play environments may no longer be accomplished using physical spaces. At-home workers and students have enjoyed needing to only dress the half of their bodies in view to the camera. Privacy concerns have led many users to create virtual backgrounds. High-quality digital imagery could easily replace our live heads with photorealistic animated headshots that do not need makeup, clothing, or lighting to make us look professionally present in classes and meetings. Populating our meetings with photorealistic avatars could have a transformative effect. Standardizing use of nonrepresentational avatars could also help organizations and communities deal with implicit biases involving race, gender, and sexual identity. After all, if "[o]n the Internet, nobody knows you're a dog"[22] applies to the metaverse, then perhaps there is some truth to the statement that "I don't see breed." This is not to suggest that all these things will come to pass or that they will all occur in the same virtual world. But they highlight the potential for a change in kind rather than degree with a fully realized metaverse.[23]

Over the course of the next months or years, most of these technological innovations will be possible. Which of these changes will be successful will turn on a number of factors, most of which will depend on the public's perception of the innovation rather than any technological merit.[24] Given the continued expansion of the video gaming industry, the societal impact of social media, and the shift to technology-mediated work and learning environments, however, it is a reasonable expectation that some of these shifts will take place,

---

21. Shisha, *supra* note 14, at 700.

22. Glenn Fleishman, *Cartoon Captures Spirit of the Internet*, N.Y. TIMES (Dec. 14, 2000), https://www.nytimes.com/2000/12/14/technology/cartoon-captures-spirit-of-the-internet.html [https://perma.cc/ARN5-6SBV] (describing the most popular cartoon licensed by *The New Yorker* magazine).

23. *See*, *e.g.*, Kenneth Rapoza, *Why you Absolutely Must Invest in the Metaverse*, FORBES (Nov. 14, 2021), https://www.forbes.com/sites/kenrapoza/2021/11/14/why-you-absolutely-must-invest-in-the-metaverse/?sh=5a0e4f23a9b0 [https://perma.cc/4MWP-3ELF].

24. *See*, *e.g.*, Lee Smith & Darienne L. Dennis, *Sony Battles Back*, FORTUNE (May 19, 2013) https://fortune.com/2013/05/19/sony-battles-back-fortune-1985/ [https://perma.cc/RAE6-BPV8] (republication of article from 1985).

creating new markets worth billions of dollars and triggering significant legal, business, and regulatory issues.

II. THE EMERGENCE OF WEB3 AND THE PHILOSOPHICAL BATTLE FOR THE METAVERSE

While this Article suggests a regulatory regime within an interoperable, ever-present metaverse, it will not be the only model to emerge. There are three primary reasons that what will emerge will be a multiverse, a loose confederation of distinct virtual worlds and metaverse environments. The multiverse will be an international, partially interoperable array of metaverses, each subject to a different mix of state authority, corporate oversight, and participatory governance.[25]

The first reason that a single metaverse will not provide a common global experience is the unique set of positive law and social norms in each country or region.[26] The governance of the internet and operation of domestic law varies considerably from country to country, and the metaverse will exacerbate rather than flatten this trend.[27] Freedom House reports, "Authorities in at least 48 countries pursued new rules for tech companies on content, data, or competition

---

25. The geopolitical and military consequences of the multiverse are beyond the scope of this Article. I have begun an exploration of this topic in a separate series of articles. *See generally* Jon M. Garon, *When AI Goes to War: Corporate Accountability for Virtual Mass Disinformation, Algorithmic Atrocities, and Synthetic Propaganda*, 49 N. KY. L. REV. 181 (2022); Jon M. Garon, *The Empires Strike Back: Reassertion of Territorial Regulation in Cyberspace*, 3 J.L. & TECH. TEX. 1 (2019); Jon M. Garon, *Cyber-World War III: Origins*, 7 J.L. & CYBER WARFARE 1 (2018).

26. *See* ADRIAN SHAHBAZ & ALLIE FUNK, FREEDOM ON THE NET: THE GLOBAL DRIVE TO CONTROL BIG TECH, FREEDOM HOUSE 1–2 (2021), https://freedomhouse.org/report/freedom-net/2021/global-drive-control-big-tech [https://perma.cc/3UAZ-M9B9]; William D. Eggers, Mike Turley, & Pankaj Kamleshkumar Kishnani, *The Future of Regulation*, DELOITTE (June 19, 2018), https://www2.deloitte.com/us/en/insights/industry/public-sector/future-of-regulation/regulating-emerging-technology.html [https://perma.cc/ZM4E-9BEW] ("The assumption that regulations can be crafted slowly and deliberately, and then remain in place, unchanged, for long periods of time, has been upended. . . . [G]overnment agencies are challenged with creating or modifying regulations, enforcing them, and communicating them to the public at a previously undreamed-of pace.").

27. *See*, *e.g.*, Mary Hui, *China is Eyeing the Metaverse as the Next Internet Battleground*, QUARTZ (Nov. 17, 2021), https://qz.com/2089316/china-sees-the-metaverse-as-the-next-internet-battleground/ [https://perma.cc/5GBE-9QFL].

> [A Chinese Government book] sketches out six major trends of the metaverse. Among them: the deep integration of the digital and real economy; data becoming a core asset; and the globalization of digital and decentralized finance, or DeFi. Those trends map neatly onto China's stated strategic goals for its internet industry and more broadly, the digital economy. The government regards data as a factor of production, and has erected a new legal infrastructure to ensure sweeping control over tech firms' data.

Id.

over the past year."[28] The U.S. regulatory model is very different from that of Europe, and even more different from the governmental control exercised in China, Russia, and by other authoritarian regimes.[29]

Secondly, the development of the metaverse or expanded metaverses comes as part of a larger movement towards Web3, the next phase in the development of the digital economy.[30] At the heart of the Web3 movement is a philosophical goal of decentralized and democratized control of the internet instead of control vesting in an oligarchic set of interdependent multinational corporations or traditional superpowers.[31] For some activities, the importance of Web3 communities and autonomy from corporate governance will drive adoption decisions. In others, the requirements of legal compliance, the importance of contractual relationships, and a risk-averse management strategy will require participation in only those aspects of the metaverse that are backed by established industry leaders that can assure compliance with regulatory requirements and product safety standards.[32]

Thirdly, as the adage notes, "The future is already here. It's just not evenly distributed yet."[33] By 2015, the importance of digital property had become so significant that the Uniform Law Commission, in partnership with the American Law Institute, adopted the Revised Uniform Fiduciary Access to

---

28. SHAHBAZ & FUNK, *supra* note 26, at 1.

29. *Id.* ("China ranks as the worst environment for internet freedom for the seventh year in a row. Chinese authorities imposed draconian prison terms for online dissent, independent reporting, and mundane daily communications.").

30. *See* Ephrat Livni, *Welcome to "Web3." What's That?*, N.Y. TIMES (Dec. 5, 2021), https://www.nytimes.com/2021/12/05/business/dealbook/what-is-web3.html [https://perma.cc/Z3JJ-U9AF].

31. *See id.*

32. This approach of risk-averse contractual partnerships was famously captured in the adage "nobody gets fired for buying IBM," a strategy that left many companies unable to pivot to the PC revolution and emergence of the internet. *See* Duena Blomstrom, *"Nobody Gets Fired for Buying IBM." But They Should.*, FORBES (Nov. 30, 2018), https://www.forbes.com/sites/duenablomstrom1/2018/11/30/nobody-gets-fired-for-buying-ibm-but-they-should [https://perma.cc/7GE8-498V]; Scott Kirsner, *The Barriers Big Companies Face When They Try to Act Like Lean Startups*, HARV. BUS. REV. ONLINE (Aug. 16, 2016), https://hbr.org/2016/08/the-barriers-big-companies-face-when-they-try-to-act-like-lean-startups [https://perma.cc/7JX8-4739].

33. Quote generally attributed to William Gibson. *See* Pagan Kennedy, *William Gibson's Future Is Now*, N.Y. TIMES (Jan. 13, 2012), https://www.nytimes.com/2012/01/15/books/review/distrust-that-particular-flavor-by-william-gibson-book-review.html [https://perma.cc/DNN4-R224] ("[T]his quote is often attributed to Gibson, though no one seems to be able to pin down when or if he actually said it. Still, it neatly sums up his own particular flavor."); s*ee also The Future Has Arrived — It's Just Not Evenly Distributed Yet*, QUOTE INVESTIGATOR (Jan. 24, 2012), https://quoteinvestigator.com/2012/01/24/future-has-arrived/ [https://perma.cc/CH9K-ZLX4] (providing an outline of the evolution of the quote with attribution to Gibson and a nod to Marshall McLuhan and Alvin Toffler).

Digital Assets Act (RUFADAA).[34] RUFADAA provides legal authority for an executor, fiduciary, or lawyer to access the account of someone who has died or become incapacitated to properly oversee the person's digital assets.[35] The law has since been adopted in all but four states, highlighting the growth in importance of digital assets.[36] As this change demonstrates, there is already too much invested in digital assets to expect that a new system will wholly or painlessly supplant what has already been adopted.

The past history of virtual worlds provides another example of the highly variable experiences to be expected. The virtual worlds of a prior decade did not actually vanish, they merely dropped out of the headlines. "Virtual reality never really left. It just shifted focus from entertainment to fields like medicine and military training."[37] The statistics for virtual worlds help provide a strong reminder that even small niche uses are significant. According to market research firm Omdia, "[I]n 2021, 12.5 million headsets will be sold, while spend on VR content will reach $2 [billion]."[38] Other reports are considerably higher, but the more moderate calculations are likely more accurate.[39]

Beyond the public interest in various tools, technologies, investments, and pastimes, there are also profound structural barriers that benefit some adopters of technology over others. "The idea of the 'digital divide' refers to the growing gap between the underprivileged members of society . . . ."[40] One simple example highlights the problem. "As more than 55 million students moved to online learning during the pandemic, one in five teens, ages 13 to 17, reported being unable to do their homework 'often' or 'sometimes' because of unreliable

---

34. *See* FIDUCIARY ACCESS TO DIGITAL ASSETS ACT, REVISED (UNIF. L. COMM'N 2018) https://www.uniformlaws.org/committees/community-home?CommunityKey=f7237fc4-74c2-4728-81c6-b39a91ecdf22 [https://perma.cc/BDG4-U7SU].

35. *Id.*; *see* S. Dresden Brunner, *Access to Digital Assets—Florida's New Law for Fiduciaries: What Are Digital Assets and Why Are They Relevant?*, FL. BAR J., Nov. 2016, at 34, 34–35, https://www.floridabar.org/the-florida-bar-journal/access-to-digital-assets-floridas-new-law-for-fiduciaries-what-are-digital-assets-and-why-are-they-relevant/ [https://perma.cc/K4R3-W9DA]; Patrick Hicks, *What is RUFADAA - Everything You Need to Know*, TRUST & WILL, https://trustandwill.com/learn/what-is-rufadaa [https://perma.cc/J6TC-27FH].

36. *See* UNIFORM LAW COMMISSION, *supra* note 34.

37. Ivan Stevanovic, *30 Virtual Reality Statistics for 2022*, KOMMANDO TECH (May 13, 2022), https://kommandotech.com/statistics/virtual-reality-statistics/ [https://perma.cc/J9Y3-WGEP].

38. George Jijiashvili, *Omdia Research Reveals 12.5 Million Consumer VR Headsets Sold in 2021 With Content Spend Exceeding $2bn*, GAME DEV. (Dec. 10, 2021), https://www.gamedeveloper.com/blogs/omdia-research-reveals-12-5-million-consumer-vr-headsets-sold-in-2021-with-content-spend-exceeding-2bn [https://perma.cc/527W-84TD].

39. Stevanovic, *supra* note 37 (reflecting 171 million active VR users in the world in 2018 with a revenue of $16.8 billion).

40. *Digital Divide*, STANFORD UNIV., https://cs.stanford.edu/people/eroberts/cs181/projects/digital-divide/start.html [https://perma.cc/RV92-9NPQ].

Internet access. Twelve million children were without internet access altogether."[41]

The digital divide disadvantages the disadvantaged, exacerbating preexisting inequities "especially [for] the poor, rural, elderly, and handicapped portion of the population who do not have access to computers or the internet; and the wealthy, middle-class, and young Americans living in urban and suburban areas who have access."[42]

> Nearly half of Americans without at-home internet were in Black and Hispanic households. With a 14-point gap in broadband access between white and Black households with school-going children, and a 12-point gap between white and Hispanic households, we find that up to 40% of disconnected K-12 students from Black, Latino, and indigenous communities struggle with insufficient digital literacy, language obstacles, and other disincentives to use the internet and find ways to gain better access.
>
> The digital divisions are likely to keep these historic disadvantages in place in the future. Seventy percent of Black and 60% of Hispanic respondents report being underprepared with digital skills, affecting their employability. While a third of all white workers in 2018 were in jobs they could do from home, less than 20% percent of Black workers and only 16% percent of Hispanic workers were in jobs that could be done remotely.[43]

The internal divides of race, poverty, and geography mean that the future development of society-changing technologies risk further reinforcing a technological caste system based on wealth, race, culture, and geography both within the U.S. and among the nations of the world. These divisions are innately inequitable for those left without access to the opportunities made uniquely through the metaverse, and they will be exploited by adversaries of the U.S. to further an anti-American narrative that paints democratic ideals as mere manipulation and propaganda.[44] For each of these three reasons, any future

---

41. Bhaskar Chakravorti, *How to Close the Digital Divide in the U.S.*, HARV. BUS. R. ONLINE (July 20, 2021), https://hbr.org/2021/07/how-to-close-the-digital-divide-in-the-u-s [https://perma.cc/34KT-RC9H].

42. STANFORD UNIVERSITY, *supra* note 40.

43. Chakravorti, *supra* note 41.

44. *See* Peter Rudolph, *The Sino-American World Conflict*, *in* SWP RESEARCH PAPER 4, STRATEGIC RIVALRY BETWEEN UNITED STATES AND CHINA 10 (Barbara Lippert & Volker Perthes eds., 2020), https://www.swp-berlin.org/en/publication/strategic-rivalry-between-united-states-and-china [https://perma.cc/V3KB-XZ5L] ("[T]he systemic conflict will loom increasingly large on the

expectations of Web3 and the metaverse must take the global competition, the varying regulatory models, and the internal inequities into account.

III. WEB3, NFTS, AND DAOS

Within the context of these three challenges, the evolution of Web3 will be particularly important to assess as it evolves over time. According to advocates of a decentralized, token-centric model of internet engagement, Web3 "will democratize everything, reshaping art, commerce and technology; displacing intermediaries; and putting people more directly in control of their destinies."[45]

Web3 differs from Web 1.0 and Web 2.0, according to analysts, in the nature of both the content and interactivity. Although the internet has been in existence since the 1970s, the modern World Wide Web or Web 1.0 was tied directly to the launch of the graphical user interface beginning with the Mozilla (Netscape) web browser in 1994.[46] In many ways, the internet of the 1990s was a digital publisher and library, dominated by content owners digitizing, organizing, and pushing out content to the public in a one-to-many model.[47] Web 2.0 was about interactivity and user generated content. "Web 2.0 refers to worldwide websites which highlight user-generated content, usability, and

American side, sometimes interpreted as a clash between 'liberal democracy' and what is occasionally referred to as 'digital authoritarianism'. Highlighting the ideological conflict might be employed to mobilise sustained domestic support for a power clash with China. . . ."); EUGENE RUMER & RICHARD SOKOLSKY, THIRTY YEARS OF U.S. POLICY TOWARD RUSSIA: CAN THE VICIOUS CIRCLE BE BROKEN? 2 (2019), https://carnegieendowment.org/2019/06/20/thirty-years-of-u.s.-policy-toward-russia-can-vicious-circle-be-broken-pub-79323 [https://perma.cc/C6LN-V7HV] ("Russian leaders see their country as a great power in charge of its own destiny. . . . [T]hey reject democracy promotion as a cover for U.S.-sponsored regime change; they . . . will resist perceived U.S. intrusions; and they rely on anti-Americanism to legitimize their unpopular policies with domestic audiences.").

45. Livni, *supra* note 30.

46. *See* Gilad Edelman, *The Father of Web3 Wants You to Trust Less*, WIRED (Nov. 29, 2021), https://www.wired.com/story/web3-gavin-wood-interview/ [https://perma.cc/FE7V-M9KL] ("Web 1.0, the story goes, was the era of decentralized, open protocols, in which most online activity involved navigating to individual static webpages."). Netscape launched in October 1994 as Mozilla and set most of the industry standards. *What Was the First Web Browser?*, STARRY (June 19, 2019), https://starry.com/blog/inside-the-internet/what-was-the-first-web-browser [https://perma.cc/C7BP-9MMH]. Tim Berners-Lee created an earlier browser in 1990. Marc Andreessen and Jamie Zawinski developed the NCSA Mosaic web browser in 1993, which became Microsoft's Internet Explorer in 1995. *Id.*

47. *See* Nupur Choudhury, *World Wide Web and Its Journey from Web 1.0 to Web 4.0*, 5 INT'L J. COMPUT. SCI. & INFO. TECH. 8096, 8096 (2014).

interoperability for end users. Web 2.0 is also called the participative social web."[48]

The generation implementing Web 1.0 started with Pong. Each node on the internet helped realize a vision of the future fostered by *Star Trek*.[49] America Online and the Yahoo! portal were groundbreaking in their day.[50] Then, with Web 2.0, the editorial power of the portals and their media-giant parent companies was disintermediated by Google's search engine and the explosion of many-to-many content that put the user's voice at the center of the media feed.[51]

For advocates of Web3, Web 2.0 shifted from its participatory roots into a centralized, algorithmically mediated new media marketplace.[52] The

48. *Comparison Between Web 1.0, Web 2.0 and Web 3.0*, GEEKSFORGEEKS (Aug. 2, 2022), https://www.geeksforgeeks.org/web-1-0-web-2-0-and-web-3-0-with-their-difference/ [https://perma.cc/47RW-5FZZ]; *see* Susannah Fox & Mary Madden, *Riding the Waves of "Web 2.0,"* PEW RSCH. CTR. (Oct. 5, 2006), https://www.pewresearch.org/internet/2006/10/05/riding-the-waves-of-web-2-0/ [https://perma.cc/S9T5-2UB4] ("[Web 2.0] provided a useful, if imperfect, conceptual umbrella under which analysts, marketers and other stakeholders in the tech field could huddle the new generation of internet applications and businesses that were emerging to form the 'participatory Web' as we know it today: Think blogs, wikis, social networking, etc.").

49. *See* Teena Maddox, *Tech Leaders Share How Star Trek Inspired Them to Pursue a Career in Technology*, TECH REPUBLIC (Jan. 23, 2020), https://www.techrepublic.com/article/tech-leaders-share-how-star-trek-inspired-them-to-pursue-a-career-in-technology/ [https://perma.cc/B9PX-3RTE].

50. *See* Edmund Lee & Lauren Hirsch, *Fortunes of AOL and Yahoo Change Again in a $5 Billion Sale*, N.Y. TIMES, May 4, 2021, at B5 ("Yahoo and AOL, kings of the early internet, saw their fortunes decline as Silicon Valley raced ahead to create new digital platforms. Google replaced Yahoo. AOL was supplanted by cable giants.").

51. *See* Paul Miller, *Web 2.0: Building the New Library*, ARIADNE (Oct. 30, 2005), http://www.ariadne.ac.uk/issue/45/miller/ [https://perma.cc/MA8H-ND43]; Scott Karp, *What Magazines Still Don't Understand About The Web*, PUBLISHING 2.0 (June 9, 2008), https://publishing2.scottkarp.ai/2008/06/09/what-magazines-still-dont-understand-about-the-web/ [https://perma.cc/GWG4-NMQS]; Choudhury, *supra* note 47, at 8099.

52. *See*, *e.g.*, Kevin Curran, *Netflix No Longer Fits in FAANG, But Here's Who Does*, THESTREET (June 7, 2021), https://www.thestreet.com/investing/netflix-no-longer-fits-in-faang-heres-who-does [https://perma.cc/ACY7-JETB] ("Nearly a decade ago, TheStreet's founder Jim Cramer coined the acronym FANG, later updated to FAANG, for companies supremely dominant in their respective markets and their stocks' resulting proclivity for outperformance."); Lara O'Reilly, *The 30 Biggest Media Companies in the World*, BUS. INSIDER (May 31, 2016), https://www.businessinsider.com/the-30-biggest-media-owners-in-the-world-2016-5 [https://perma.cc/DAE5-TFKN] ("Digital giants are increasingly dominating the global advertising market. In 2015, Google, Facebook, Baidu, Yahoo, and Microsoft accounted for 19% of all the global ad spend flowing through all media, according to media agency ZenithOptimedia's 2016 'Top Thirty Global Media Owners' report."); Florian Saurwein & Charlotte Spencer-Smith, *Automated Trouble: The Role of Algorithmic Selection in Harms on Social Media Platforms*, 9 MEDIA & COMM. 222, 222 (2021) https://www.cogitatiopress.com/mediaandcommunication/article/view/4062 [https://perma.cc/2ZCU-LYWB].

dominance of the FAANG companies—Facebook, Apple, Amazon, Netflix, and Google—largely undermine the ethos of Web 2.0 as being about individual participation. While Facebook, YouTube, TikTok, Twitter, and others are about user content, the role of algorithms to manage what one sees, and the dominance of the platforms, make the internet feel very ownership centric. Naval Ravikant tweeted, "Web 2: Users are the data, corporations own the platform, and the code is closed. Web 3: Users own their data, contributors own the platform, and the code is open."[53]

"Web 2.0, which we're living through now, is the era of centralization, in which a huge share of communication and commerce takes place on closed platforms owned by a handful of super-powerful corporations—think Google, Facebook, Amazon—subject to the nominal control of centralized government regulators."[54] Combined with powerful centralized control enforced through the terms of service, Web 2.0 is publicly perceived as a digital industrial age dominated by massive multinational corporations.[55] Even though more than 80% of the public uses YouTube and nearly 70% of the public uses Facebook, the era is known for the corporate management of public content rather than the

---

> Evidence of harms involving social media algorithms was collected from media reports and academic papers within a two-year timeframe from 2018 to 2019, covering Facebook, YouTube, Instagram, and Twitter. Harms with similar casual mechanisms were grouped together to inductively develop a typology of algorithmic harm based on the mechanisms involved in their emergence: (1) algorithmic errors, undesirable, or disturbing selections; (2) manipulation by users to achieve algorithmic outputs to harass other users or disrupt public discourse; (3) algorithmic reinforcement of pre-existing harms and inequalities in society; (4) enablement of harmful practices that are opaque and discriminatory; and (5) strengthening of platform power over users, markets, and society.

Id.

53. Naval Ravikant (@naval), TWITTER (Oct. 12, 2021, 7:52 PM), https://twitter.com/naval/status/1448089151677603846 [https://perma.cc/BDQ9-VN86].

54. Edelman, *supra* note 46.

55. *See*, *e.g.*, In Song Kim & Helen v. Milner, Multinational Corporations and their Influence Through Lobbying on Foreign Policy 8–9 (Dec. 2, 2019), https://www.brookings.edu/wp-content/uploads/2019/12/Kim_Milner_manuscript.pdf [https://perma.cc/K3Y5-U5P6] ("[R]esearch on business political activity is that large firms lobby the most. . . . Moreover, larger firms utilize their resources to actually spend more. . . . The biggest firms are also able to leverage considerable informational advantages . . . which help to reduce uncertainty for policymakers.") (citations omitted); *Global Implications of Media and Technology*, LUMEN LEARNING, https://courses.lumenlearning.com/sociology/chapter/global-implications-of-media-and-technology/ [https://perma.cc/DT4S-YR53] ("On the surface, there is endless opportunity to find diverse media outlets. But the numbers are misleading. . . . In 1983, a mere 50 corporations owned the bulk of mass-media outlets. Today in the United States . . . just five companies control 90 percent of media outlets.") (citation omitted).

decentralized nature of media.[56] Despite the participation by the public, Web 2.0 revenue is driven by advertising.[57]

Web3, its evangelists predict, will use the power of digital property to empower the individual.[58] "For Web3, the internet is shifting from ad-based business models to *commerce*-based business models. . . . As the internet evolves, it becomes more participatory. People move from passive consumers to active creators."[59] Gavin Wood, founder of the Web3 Foundation, has been quoted as explaining, "Web3 is actually much more of a larger sociopolitical movement that is moving away from arbitrary authorities into a much more rationally based liberal model. And this is the only way I can see of safeguarding the liberal world . . . ."[60]

The question remains whether this vision is different than the vision of earlier Web 1.0 and Web 2.0 advocates regarding their model of an internet.[61] John Perry Barlow chided the "Governments of the Industrial World" that "[y]ou claim there are problems among us that you need to solve. . . . Many of these problems don't exist."[62] The earlier utopian idea failed and created a vacuum into which U.S. corporations were able to bestride the narrow world, each like a mighty colossus.[63]

---

56. Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, PEW RSCH. CTR. (Apr. 7, 2021), https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/ [https://perma.cc/65H7-5D8X] (reporting that 81% of Americans use YouTube and 69% use Facebook).

57. Rex Woodbury, *Chain Reactions: How Creators, Web3, and the Metaverse Intersect*, DIGIT. NATIVE (May 5, 2021), https://digitalnative.substack.com/p/chain-reactions-how-creators-web3 [https://perma.cc/KQU4-FQA6] ("Most big Web1 and Web2 companies make money through advertising.").

58. *See* Edelman, *supra* note 46 ("Gavin Wood coined the term Web3 (originally Web 3.0) in 2014. At the time, he was fresh off of helping develop Ethereum, the cryptocurrency that is second only to Bitcoin in prominence and market size.").

59. Woodbury, *supra* note 57 (emphasis in the original).

60. Edelman, *supra* note 46.

61. *See* John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence [https://perma.cc/KS7U-BFGM] ("Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone.").

62. *Id.*

63. *See* WILLIAM SHAKESPEARE, JULIUS CAESAR act 1, sc. 2, l. 136–42.

> CASSIUS
> Why, man, he spans this narrow world
> like the Colossus, and we puny men
> Walk under his huge legs, and peep about
> To find ourselves dishonorable graves.

Like the earlier generation of anti-regulators, the current Web3 enthusiasts tend to ignore both the nature of the people who actively used the technologies and the people left without access to its benefits. But the increasingly lower barriers to entry for creation and economic opportunity in the Web3 economy should at least reduce these disparities.[64]

Moreover, at the same time there is a strong diffusion of wealth and power away from the U.S. In 2012, the National Intelligence Council published a global trend analysis to review the likely shifts in the coming two decades.[65] The report provided some prescient scenarios of the world of 2030:

> In the most plausible worst-case scenario, the risks of interstate conflict increase. The U.S. draws inward and globalization stalls.
>
> . . . .
>
> Inequalities explode as some countries become big winners and others fail. Inequalities within countries increase social tensions. Without completely disengaging, the U.S. is no longer the "global policeman."
>
> Driven by new technologies, nonstate actors take the lead in confronting global challenges.[66]

Reading the predictions at their halfway point, the first two predictions have come to pass, leading advocates for Web3 to embrace nonstate actors as a solution. Evangelists for Web3 point out that these changes are already occurring. There is over $2.3 trillion in value that has accrued in the thousands of cryptocurrencies that have emerged in the past five years.[67] This demonstrates a tremendous global demand for non-fiat currencies. That demand may also reflect the interest by some asset holders of their need to move out of

---

> Men at some time are masters of their fates.
> The fault, dear Brutus, is not in our stars,
> But in ourselves, that we are underlings.

Id.

64. *See* Woodbury, *supra* note 57 ("More broadly, it's easier than ever to build *companies*. Amazon Web Services and Stripe are Lego-like building blocks that make it fast and easy to launch a business. Software is becoming more accessible to use, allowing anyone to be a creator entrepreneur.").

65. NATIONAL INTELLIGENCE COUNCIL, GLOBAL TRENDS 2030: ALTERNATIVE WORLDS i (2012), https://www.dni.gov/files/documents/GlobalTrends_2030.pdf [https://perma.cc/SP45-HK3D].

66. *Id.* at ii.

67. Livni, *supra* note 30 ("At the start of 2020, a Bitcoin was worth just over $7,000. Today, it's trading at about $50,000, and the value of all cryptocurrencies, of which Bitcoin is one among many, is some $2.3 trillion.").

unstable economies, to avoid government regulation, or some combination of both.[68]

Goldman Sachs suggests that key elements of this model will emerge. It provides a few key principles:

> [1] Likely more control by the user of their data (including data residing on-device);
> [2] Likely a more micro focus - a mean reversion on scale (either in end market being tackled or in relationship between the platform and the user);
> [3] The rise of individual as creator & creator monetizing their content more directly with "fans";
> [4] Increasingly decentralized (with the possible breakdown of the mobile operating system/app store distribution model over the next 5-10 years); &
> [5] Flexibility (if not innovation) on payment mechanisms aimed at a mix of themes, including decentralized privacy and anti-establishment.[69]

These are not particularly bold predictions since they largely describe the nascent Web3 economy of 2021. In the last few years, for example, blockchain technologies have expanded into multiple areas beyond cryptocurrency. The most popular expansion of blockchain technology has been through the collection, sale, and trading of nonfungible tokens (NFTs). "So far in 2021, about $27 billion worth of crypto has been spent on major NFT platforms, according to Chainalysis. That's up from $114 million in all of last year."[70]

The use of NFTs creates a mechanism for digital assets to be uniquely identified, provided a nearly unforgeable provenance, and be available for

---

68. *See, e.g.*, Werner Vermaak, *Afghanistan: Can Blockchain and Crypto Prevent or Mitigate The Fallout of Failing States?*, ALEXANDRIA, https://coinmarketcap.com/alexandria/article/afghanistan-can-blockchain-and-crypto-prevent-or-mitigate-the-fallout-of-failing-states [https://perma.cc/PF9J-AT36] ("El Salvador's recent decision to adopt Bitcoin as a national currency could improve their economy by easing money transfers from El Salvadorians abroad and providing financial services to locals who can't otherwise afford them. The same technology would have proved exceedingly useful during the Taliban's recent run on the banks."); Cady Voge, *Where Could Bitcoin Succeed as a Currency? In a Failed State*, WIRED (Mar. 22, 2018), https://www.wired.com/story/where-could-bitcoin-succeed-as-a-currency-in-a-failed-state/ [https://perma.cc/EBS8-QULW] ("[I]n Venezuela, where inflation topped 2,616 percent last year, cryptocurrency is a way around restrictions on holding foreign currency, and in some cases, a means of survival."); Cynthia Dion-Schwarz, David Manheim & Patrick B. Johnston, TERRORIST USE OF CRYPTOCURRENCIES - TECHNICAL AND ORGANIZATIONAL BARRIERS AND FUTURE THREATS 14 (2019) https://www.rand.org/pubs/research_reports/RR3026.html [https://perma.cc/7U5N-N3JE] ("The question of whether and how terrorist organizations would use a cryptocurrency system depends on the available technology and its properties, as well as the groups' needs and capabilities.").

69. SHERIDAN, *supra* note 6, at 3.

70. Livni, *supra* note 30.

trading, largely without the need for large, centralized intermediaries.[71] The NFT is more than just simply a digital certificate of authenticity, however, because it typically includes code that specifies conditions of ownership and transfer. These provisions are unfortunately and inaccurately labeled "smart contracts,"[72] though they can more accurately be described as automated provisions for digital transactions. "Smart contracts are open-sourced blockchain protocols that directly control the transfer of digital currencies or assets between parties under certain terms and conditions."[73] For current internet users, NFTs provide a fundamentally new way of approaching ownership of digital assets, since those had previously been defined by the terms of service rather than property law.[74] For those involved in Web 1.0, the use of NFTs is quite analogous to the early efforts in copyright law to provide digital protections measures for digital assets, micropayment systems, and other property-oriented approaches to protect artists and individuals from corporate overreach.[75] Social trends and the digital native culture, however, may create a different outcome in Web3 than that which occurred in Web 1.0.

> We're becoming a digital-first species, and at the same time we're rejecting institutions. Those two factors are combining to make work more disaggregated and creative, fueling the

71. *See* Pratin Vallabhaneni, *The Rise of NFTs – Opportunities and Legal Issues*, WHITE & CASE (Apr. 20, 2021), https://www.whitecase.com/publications/alert/rise-nfts-opportunities-and-legal-issues [https://perma.cc/8GER-DDQA] ("[A]n NFT . . . contains a unique identification code and metadata that distinguishes one NFT from any other, and represents items on the blockchain that cannot be replicated. . . . Moreover, NFTs are composed of software code in the form of 'smart contracts' that can be crafted to provide significant benefits to NFT creators.").

72. Quinn Dupont & Bill Maurer, *Ledgers and Law in the Blockchain*, KINGS REV. (June 23, 2015), https://www.kingsreview.co.uk/essays/ledgers-and-law-in-the-blockchain [https://perma.cc/8CN5-Z3TT] ("[S]mart contracts seem to miss the whole point of contracts: that, like promises, they are made to be broken. . . . Contracts, by contrast, are all about managing uncertainty."). Smart contracts are merely short code, often containing programming errors made immutable in the blockchain. David G.W. Birch, *They're Not Smart And They're Not Contracts*, FORBES (Sept. 4, 2021), https://www.forbes.com/sites/davidbirch/2021/09/04/theyre-not-smart-and-theyre-not-contacts/?sh=3b0db44a397e [https://perma.cc/7LBY-VJ34]. Companies treating the use of these coding errors as hacking, therefore, acknowledge that the terms of the contract are likely not the same as the code in the token. *Id.* "Ethereum inventor Vitalik Buterin[ ] comment[ed] that he wished that with hindsight he had used the word 'persistent script' instead." *Id.*

73. Vallabhaneni, *supra* note 71.

74. *See generally* JOSHUA FAIRCHILD, OWNED: PROPERTY, PRIVACY, AND THE NEW DIGITAL SERFDOM (2017). Since the focus of this Article is on the metaverse, the discussion of Web3 will be limited to its intersection with virtual world architectures. The broader implications of the Web3 will be addressed separately.

75. *See* Jon M. Garon, *What If DRM Fails?: Seeking Patronage in the iWasteland and the Virtual O*, 2008 MICH. ST. L. REV. 1, 27–30 (2008) (discussing the economic hardship on individual artists and predicting a return to patronage systems of artistic support).

> creator economy and letting everyone build with technology. Web3 and new business models will better allow creators and their communities to capture and exchange value, forming robust digital economies. Ultimately, this will lead to an immersive, decentralized metaverse.[76]

The demographic shifts,[77] changes in technologies, and the central role the internet now plays in many people's daily lives all suggest the transformation will take place. Despite these changes, however, that does not suggest that governments are prepared to sit back or that established enterprises are not going to find strategies to dominate the emerging markets.

In the context of cryptocurrency, for example, each sovereign state will determine the degree to which it is willing to have a non-fiat currency compete with the nation's fiat currency, the extent to which the use of the public is in need of consumer protection regulation, and the degree to which the marketplace for these assets must be regulated to control fraud and abuse.[78] The choices will likely vary from country to country, and they may also vary considerably depending on the particular attributes of each cryptocurrency.

The power of the FAANG companies have led proponents of Web3 to embrace a similar, libertarian ethos against organizational management. This movement can best be seen in the popularity of Decentralized Autonomous Organizations (DAOs).

> DAOs . . . unlock radically new ways to organize capital and human resources. Packy McCormick sums it up succinctly: "DAOs are a new way to finance projects, govern communities, and share value. Instead of a top-down hierarchical structure, they use Web3 technology and rapidly evolving governance and incentive systems to distribute decision-making authority and financial rewards. Typically, they do that by issuing tokens based on participation, contribution, and investment. Token holders then

---

76. Woodbury, *supra* note 57 ("As a 90s kid, I'll never forget loitering in the food court with friends . . . . The mall was the hub around which our social lives revolved. Today's kids hang out on Snapchat, on TikTok, in Roblox, in Fortnite. The internet is the new place to be.").

77. *See id.* ("In 2010, there were 2 billion people online—about 30% of the world's population. Over the last decade, that's swelled to 4.5 billion people and 60% of the world.").

78. *See* Robert Litan, *Regulation*, LIBR. OF ECON. & LIBERTY, https://www.econlib.org/library/Enc/Regulation.html [https://perma.cc/G7QT-4N3Y] (highlighting disclosure requirements, antitrust and competition laws, safety, and taxes as the purposes of regulation); *Objectives of Market Regulation*, ANALYSTPREP (Sept. 12, 2019), https://analystprep.com/cfa-level-1-exam/equity/objectives-market-regulation/ [https://perma.cc/JT49-967T] ("The objectives of market regulation are to control fraud, control agency problems, promote fairness, set mutually beneficial standards, prevent undercapitalized financial firms from making excessively risky investments, and to ensure that long-term liabilities are funded.").

> have the ability to submit proposals, vote, and share in the upside."[79]

DAOs can be analogized to nonprofit membership organizations which have no professional staff, to share ownership in corporations, or to labor unions which own their companies. The DAOs will be one potential model for governance of the metaverse—or at least some games and virtual worlds that connect into the metaverse. It is hard not to reflect that history has attempted this revolution before or to ignore that "[a]ll animals are equal, but some animals are more equal than others."[80] Tokens will be meted out based on payment, proof of work, or some other system. The attention span to provide governance from below will not be evenly distributed. Like political movements, some DAOs will be captured by their fringe elements. Others will be operated by those who are most expert at gathering the resources from the broader community. Still others are likely to be built with advantages for the founders, much like or even stronger than the venture-capital-backed publicly traded corporations of today. Ironically, it should not be forgotten that a stock certificate is precisely a token of distributed ownership designed to allow aggregation of capital, liquidity, and shared governance.

For some organizations and for particular purposes, however, the DAO may be an appropriate operational approach.[81] Just as there are nonprofits, public benefit corporations, limited liability companies, and close corporations to serve as alternatives to the Chapter C corporation, there will be times that DAOs are best suited to the public's interest in a particular cause, enterprise, or entertainment.

For the limited purpose of addressing the metaverse, however, there is a clear battle brewing between the centralized vision of a virtual world network organized and managed by Meta and other FAANG companies or a series of open-source protocols utilized through the sharing of NFTs and the smart contract rules associated with those tokens. The existing exemplars of the metaverse are predominantly controlled by centralized corporations and

---

79. Yash Bagal, *How Web3 Redefines Labour, Capital, and Fandom in Music*, APPETITE FOR DISTRACTION (Dec. 6, 2021), https://yashbagal.substack.com/p/web3-daos-nfts-music-creators [https://perma.cc/G8EP-XHQK]; *see* Brandon Echter, *Crypto and the metaverse with Packy McCormick of Not Boring*, SOLANA (Oct. 12, 2021), https://solana.com/news/packy-mccormick-of-not-boring-on [https://perma.cc/F6XT-RLM3] (quoting Packy McCormick, writer, NOT BORING) ("One of the things I think crypto does well is give physical-ish characteristics to digital things, and so I think a interface that makes that clear will have a lot of value in just making a lot of the stuff that feels a little more ethereal feel more real and tangible. . . .").

80. GEORGE ORWELL, ANIMAL FARM 88 (Alfred A. Knopf Inc. ed. 1989).

81. *See* Dave Rodman, *DAOs: A Legal Analysis*, JD SUPRA (Apr. 1, 2021), https://www.jdsupra.com/legalnews/daos-a-legal-analysis-6177928/ [https://perma.cc/U2R9-778B].

carefully curated. These include *Roblox*, *Fortnite*, and Microsoft's *Minecraft*.[82] These companies also adhere to restrictions of the Children's Online Privacy Protection Act requiring additional protections for minors under the age of thirteen.[83]

In contrast, there are NFT-based metaverse projects that seek to remove corporate ownership (or at least remove the FAANG companies from the list of corporate owners) and replace centralized control with user-based or community-based control. One such project is Decentraland.[84] It is operated by the Decentraland Foundation operating on behalf of the community DAO.[85] Although a DAO, it has community committees, such as the "wearables curation committee" to establish certain acceptable standards within the community.[86] Another of the significant noncentralized metaverses is Sandbox.[87] "Sandbox is a virtual world made-up of NFTs (LANDS, ASSETS, GAMES). Meaning, users have absolute ownership of their creations and LANDs in the Metaverse. For that reason, the Sandbox Metaverse is a promising investment area."[88] Both Sandbox and Decentraland rely on the Ethereum platform for their NFT operating network.[89]

Neither the centrally operated metaverses nor the NFT/DAO metaverses will be able to eradicate the other, and in some areas, there may even be

82. *See* Yao Du, Thomas D. Grace, Krithika Jagannath & Katie Salen-Tekinbas, *Connected Play in Virtual Worlds: Communication and Control Mechanisms in Virtual Worlds for Children and Adolescents*, MULTIMODAL TECH. & INTERACTIONS May 2021, at 1, 15 (2021), https://www.mdpi.com/2414-4088/5/5/27/pdf [https://perma.cc/P785-WQC5] (discussing parental controls and moderation is a wide range of platforms).

83. *Id.* at 7–8.

84. *See* Alexandra Marquez, *Welcome to Decentraland, Where NFTs Meet a Virtual World*, NBC NEWS (Apr. 3, 2021), https://www.nbcnews.com/tech/tech-news/welcome-decentraland-nfts-meet-virtual-world-rcna553 [https://perma.cc/UFW5-WYUT] ("Most everything in Decentraland is an NFT, from its virtual plots of land to the art on the walls in the virtual galleries. Ownership also gives users a say in how the virtual world operates.").

85. DECENTRALAND, *Terms of Use*, https://decentraland.org/terms/ [https://perma.cc/5459-YWHT].

86. *Id*.

87. *See* Sébastien Borget, *The Sandbox (SAND): Tokenized Assets for Gaming Ecosystems*, CRYPTOPEDIA (Dec. 23, 2021), https://www.gemini.com/cryptopedia/the-sandbox-sand-crypto-nft-virtual-world [https://perma.cc/Z7EN-J8JM] (post by the Sandbox Co-Founder & COO) ("The Sandbox is an Ethereum-based metaverse and gaming ecosystem where users can create, share, and monetize in-world assets and gaming experiences. . . . The Sandbox is designed to disrupt the traditional gaming market in which platforms own and control user-generated content whereby the rights of creators and gamers are limited.").

88. Melwyn Joseph, *Sandbox Metaverse: Is The Sandbox Playable and Is The Sandbox An NFT?*, STEALTH OPTIONAL (Dec. 6, 2021), https://stealthoptional.com/metaverse/sandbox-metaverse-is-the-sandbox-playable-and-is-the-sandbox-an-nft/ [https://perma.cc/XDT8-5MLJ].

89. *Id.*; DECENTRALAND, *supra* note 85.

cooperation. Nonetheless, control of the metaphorical capital cities within the metaverse and the key economic assets could well be worth trillions of dollars. The competition between the Fortune 50 companies and newly formed DAOs will shape the internet for the next generation.

IV. A GLIMPSE OF THE U.S. LEGAL ROADMAP

The expansion of virtual worlds will take place within an environment largely defined by intellectual property rights of copyright, trademark, patent, trade secret, and publicity rights,[90] as well as the digital property rights associated with NFTs and their smart contracts. Other than for the NFTs, each of these doctrines is well established, making it likely that the application of these intellectual property rights will be generally predictable within the metaverse environment. Beyond the intellectual property regime, however, there may be some areas where the expansion of virtual worlds to large-scale adoption of a metaverse will have unanticipated implications and complications.

Unlike the "real" world, the interactions within the metaverse are framed by contractual relations between the site owner and the participants in which the contractual agreements and terms of service take on an extremely important role. There have been numerous examples of users on platforms challenging the enforceability of end user license agreements or terms of service agreements.[91] When the host is a gaming company, such questions are generally treated as simple contract issues.[92] But if the use of virtual worlds develops into "The Metaverse," a single, ubiquitous platform or an interconnected series of commercially owned platforms, then the market power of the host will raise additional questions regarding the unconscionability of any terms imposed by the all-powerful system owner, the potential to treat the platform as a common

90. *See*, *e.g.*, E.S.S. Ent. 2000, Inc. v. Rock Star Videos, Inc., 547 F.3d 1095, 1097–98, 1101 (9th Cir. 2008) (trademarks); Hart v. Elec. Arts, Inc., 717 F.3d 141, 145, 170 (3d Cir. 2013) (publicity rights); Brown v. Entm't Merchs. Ass'n, 564 U.S. 786, 788–91, 856 (2011) (free speech rights); Pellegrino v. Epic Games, Inc., 451 F. Supp. 3d 373, 383, 385 (E.D. Pa. 2020) (false endorsement); Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510, 1514, 1527–28 (9th Cir. 1992) (copyright); National Basketball Ass'n v. Motorola, Inc., 105 F.3d 841, 844–46 (2d Cir. 1997) (copyright); *see also* Sophie Goossens, Christine Morgan, Cem Kuru, Fred Ji & DJ Cespedes, *Protecting Intellectual Property In The Metaverse*, 33 INTELL. PROP. & TECH. L.J. 11, 11–12, 14–16 (2021); Barlow, *supra* note 61; Jessica Litman, *Imaginary Bottles*, 18 DUKE L. & TECH. REV. 127, 128–29 (2019); Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 534–37 (2003).

91. *E.g.*, MDY Indus., LLC v. Blizzard Ent, Inc., 629 F.3d 928, 935, 938–39 (9th Cir. 2010); Bragg v. Linden Rsch., Inc., 487 F. Supp. 2d 593, 606–07 (E.D. Pa. 2007); *see also* Kevin Carr, *Digital Assets & License Protections in an Age That Denies Class Actions and Mandates Arbitration*, 2021 J. DISP. RESOL. 335, 336 (2021).

92. *E.g.*, *Blizzard Ent, Inc.*, 629 F.3d at 939, 941; *Linden Rsch., Inc.*, 487 F. Supp. 2d at 605.

carrier, or to redefine and regulate the environment to avoid unfair and deceptive trade practices.[93]

To the extent the metaverse is used by governmental agencies, then the spaces operated and managed by the government might be considered to become designated public fora within the proprietary metaverse.[94] Further distinctions may be needed when a government official is acting in a private, nongovernmental capacity from the person's actions in an official capacity.[95]

---

93. *See* Biden v. Knight First Amend. Inst. at Columbia Univ., 141 S. Ct. 1220, 1220 (2021) (granting cert. and vacating lower court decision as moot). In his concurrence to the dismissal of the certiorari petition, Justice Thomas made this point:

> The analogy to common carriers is even clearer for digital platforms that have dominant market share. Similar to utilities, today's dominant digital platforms derive much of their value from network size. The Internet, of course, is a network. But these digital platforms are networks within that network. . . .
>
> . . . .
>
> Much like with a communications utility, this concentration gives some digital platforms enormous control over speech. When a user does not already know exactly where to find something on the Internet—and users rarely do—Google is the gatekeeper between that user and the speech of others 90% of the time. It can suppress content by deindexing or downlisting a search result or by steering users away from certain content by manually altering autocomplete results. . . . Facebook and Twitter can greatly narrow a person's information flow through similar means. And, as the distributor of the clear majority of e-books and about half of all physical books, Amazon can impose cataclysmic consequences on authors by, among other things, blocking a listing.
>
> . . . .
>
> If the analogy between common carriers and digital platforms is correct, then an answer may arise for dissatisfied platform users who would appreciate not being blocked: laws that restrict the platform's right to exclude.
>
> . . . .
>
> None of this analysis means, however, that the First Amendment is irrelevant until a legislature imposes common carrier or public accommodation restrictions—only that the principal means for regulating digital platforms is through those methods.

Id. at 1224–26 (Thomas, J., concurring) (citations omitted).

94. *See, e.g.*, Knight First Amend. Inst. at Columbia Univ. v. Trump, 928 F.3d 226, 237 (2d Cir. 2019), *dismissed as moot*, Biden v. Knight First Amend. Inst. at Columbia Univ., 141 S. Ct. 1220, 1220 (2021); Davison v. Randall, 912 F.3d 666, 685 (4th Cir. 2019); *see also* Adam Candeub, *Bargaining for Free Speech: Common Carriage, Network Neutrality, and Section 230*, 22 YALE J. L. & TECH. 391, 399 (2020) ("[C]ommunications regulation, particularly common carriage, has always encompassed more than antitrust because communications networks offer essential public goods.").

95. *See* Lindke v. Freed, 563 F. Supp. 3d 704, 710 (E.D. Mich. 2021) ("Courts have approached this argument by examining whether the public official acted under color of state law in maintaining the social media account, thereby triggering First Amendment concerns.").

A. State Regulation Through Gambling Laws

As the metaverse grows more robust in user experience and the Web3 expectations of participatory creative ownership, it must serve as a marketplace for commercial transactions. Transactions involving only in-world digital assets will be predominantly regulated with reference to the terms of service required of all metaverse participants.[96] If the world uses in-game currency, then transactions are unlikely to trigger significant regulatory scrutiny. Even here, however, there are variations among different state laws. In *Kater v. Churchill Downs, Inc*.,[97] the Ninth Circuit recently interpreted Washington State's Recovery of Money Lost at Gambling Act (RMLGA)[98] very broadly. The court explained:

> [Virtual chips] permit a user to play the casino games inside the virtual Big Fish Casino. . . . Without virtual chips, a user is unable to play Big Fish Casino's various games. Thus, if a user runs out of virtual chips and wants to continue playing Big Fish Casino, she must buy more chips to have "the privilege of playing the game."[99]

As a result, the plaintiff—and the 50,000 others who later joined the class action—had the right to recover their losses in the game.[100]

---

96. *See infra* Section V.A. (discussing terms of service requirements). *But see* João Marinotti, *Tangibility as Technology*, 37 GA. ST. U. L. REV. 671, 713–14 (2021) (noting that real property, bailment and similar legal doctrines are not subject to contractual waivers and will take precedence over attempts to limit liability by contract).

97. Kater v. Churchill Downs Inc., 886 F.3d 784, 786 (9th Cir. 2018).

> "Gambling" is defined as the "[1] staking or risking something of value [2] upon the outcome of a contest of chance or a future contingent event not under the person's control or influence, [3] upon an agreement or understanding that the person or someone else will receive something of value in the event of a certain outcome."

Id. (quoting Wash. Rev. Code § 9.46.0237 (2005)).

98. Wash. Rev. Code § 4.24.070 (1957).

> All persons losing money or anything of value at or on any illegal gambling games shall have a cause of action to recover from the dealer or player winning, or from the proprietor for whose benefit such game was played or dealt, or such money or things of value won, the amount of the money or the value of the thing so lost.

Id.

99. *Kater*, 886 F.3d at 787; s*ee* James Gatto & Mark Patrick, *How the Evolution of Games Has Led to a Rise in Gambling Concerns: All Bets are On! Gambling and Video Games*, NAT. L. REV. (Sept. 16, 2018), https://www.natlawreview.com/article/how-evolution-games-has-led-to-rise-gambling-concerns-all-bets-are-gambling-and [https://perma.cc/R4MX-SW2R].

100. Peter Hayes, *Churchill Downs, Others Settle Gaming App Suit for $155 Million*, BLOOMBERG L. (Feb. 12, 2021), https://news.bloomberglaw.com/class-action/churchill-downs-others-settle-gaming-app-suit-for-155-million [https://perma.cc/K7VN-JMFK].

When game assets can be converted to cash, in-world wagering typically meets the three-pronged test of (1) payment of some form of consideration, (2) a result determined by chance rather than skill, (3) resulting in the award of a prize.[101] "While these three elements seem to be fairly simple terms, their interpretation is not. Their meaning varies from state to state."[102] As the metaverse expands, the potential for in-world assets to become exchangeable for other things of value increases, meaning the prize becomes far more important when a game is tied to the interoperability of the metaverse or two exchangeable assets.

While most states may not treat in-game assets as illegal gambling when used only for in-game play, if the in-game currency can be converted to money or items of value, then game publishers and metaverse operators must address the unintended additional legal implications.[103] The lesson of *Kater* should not be lost on Web3 architects. A relatively minor definitional construction in a state gambling statute was enough to undermine a longstanding, robust online business model. If states become frustrated with a loss of tax revenue, regulatory control, or impotent consumer protection laws, they can easily amend domestic laws to turn NFTs and in-game assets into regulated casino chips, thereby imposing costly state liabilities on transactions previously thought to be immune.[104]

B. Federal Regulation Through Money Transfer, Securities and Foreign Investment Laws

Transferring funds or fungible assets within the game or world will be subject to money transfer laws if the funds can be converted to currency, assets,

---

101. Gatto & Patrick, *supra* note 99 ("In general, if all three of these elements are present, that offering may be an illegal lottery and may also constitute illegal gambling. If at least one of these elements is removed, the offering will generally fall outside the anti-lottery/gambling laws.").

102. *Id.*

103. *See*, *e.g.*, Paul C. Nylen, *Imposing a Deadline on the IRS: Artificial Intelligence Tries to Beat "Starcraft" While the IRS Tries to Regulate Virtual Currency*, 52 AKRON L. REV. 945, 953–54 (2019) (addressing tax obligation and foreign bank reporting obligations); Nika Antonikova, *Real Taxes on Virtual Currencies: What Does the I.R.S. Say?*, 34 VA. TAX REV. 433, 441–42 (2015) ("A taxpayer who receives virtual currency must include the fair market value of the virtual currency in computing gross income both if currency was received in exchange for goods and services, and if it was 'mined' by a taxpayer."); Sean F. Kane, *Virtual Worlds, Digital Economies, and Synthetic Crimes*, PRAC. LAW., Apr. 2008, at 35, 44 ("With such freedom of unregulated and unreported access and transfer, as being offered first by *Entropia Universe's* accounts, the Money Laundering Control Act will be difficult to fully enforce.").

104. *See Kater*, 886 F.3d at 787.

or crypto.[105] To the extent that virtual worlds are in the money-services business as a function of the platform's ability to exchange in-world digital assets for fiat currency or cryptocurrency, then the platform will need to register as a money-services business.[106] *Second Life* has taken that step for its own operations and more recently for its users.[107] In-game banking and investment services will likely be subject to the regulations governing real-world activities.[108] Depending on the financial transactions that can occur within the

105. *See* Currency and Foreign Transactions Reporting Act, Pub. L. No. 91-508, 84 Stat. 1118 (1970), 18 U.S.C § 1956 (2018) (Bank Secrecy Act); *see also* Stan Sater, *Do We Need KYC/AML: The Bank Secrecy Act and Virtual Currency Exchanges*, 73 ARK. L. REV. 397, 417, 422 (2020); Anton Moiseienko & Kayla Izenman, *Gaming the System: Money Laundering Through Online Games*, RUSI NEWSBRIEF, Oct. 2019, at 1, 3 https://rusi.org/explore-our-research/publications/rusi-newsbrief/gaming-system-money-laundering-through-online-games [https://perma.cc/VJW9-GRCL] ("If a computer game allows players to transfer in-game items to each other, and these in-game items can be exchanged into fiat currency, the gaming company's position is similar to that of a virtual currency exchange. But unlike gaming companies, virtual currency exchanges should be subject to [anti-money laundering regulations].").

106. *See* 18 U.S.C. § 1960(a)(2) ("[T]he term 'money transmitting' includes transferring funds on behalf of the public by any and all means including but not limited to transfers within this country or to locations abroad by wire, check, draft, facsimile, or courier. . . ."); Sater, *supra* note 105, at 398–99.

> In 2013, FinCEN published guidance titled Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies (2013 Guidance). The 2013 Guidance interpreted the BSA Regulations and contextualized them to the virtual currency ecosystem while also inventing new terms such as "user," "exchanger," "administrator," "virtual currency," and "convertible virtual currency." In subsequent guidance and administrative rulings, FinCEN regularly uses these terms as well as defining new terms to continually apply the BSA Regulations to different business models that are of note in the virtual currency ecosystem.

Id. (quoting U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES 1 (2013)).

107. Moiseienko & Izenman, *supra* note 105, at 3.

> On 1 July 2019, Linden Lab, the developer of the online game *Second Life*, announced that all *Second Life* users would henceforth need to register with its fully owned subsidiary Tilia Inc., a money service business (MSB) licensed in 46 US states. As an MSB, Tilia is required to comply with AML/CTF obligations under the Bank Secrecy Act and its implementing regulations, including in relation to customer verification and suspicious transaction reporting.

Id.

108. *See* James P. Brennan, Joshua McDougall, Eric Hornung, Seth Litwack & Madiha Zuberi, *The Curious Case of Crypto*, BANKING & FIN. SERVS. POL'Y REP., Apr. 2018, at 8, 12 (discussing state money transfer registration requirements in Washington and New York).

game or virtual world, potentially every financial regulatory body could claim jurisdiction over some aspect of these financial transactions.[109]

i. Money Transfer Regulations

There is a strong appetite for cryptocurrencies, but the need case may not fully match the interest. "Despite the much-touted economic, political, and ideological motivations behind the creation of cryptocurrencies, they have emerged to address market frictions."[110] Prior to the emergence of cryptocurrency, "Commerce on the Internet [had] come to rely almost exclusively on financial institutions serving as trusted third parties to process electronic payments. While the system works well enough for most transactions, it still suffers from the inherent weaknesses of the trust based model."[111] The profitability of the trust model, after all, is built on "the absence of complete trust between parties . . . [which] imposes costs on both institutions and consumers, including contracting, search, and verification costs."[112] Decentralized finance (DeFi) offers a solution to improve trust and therefore reduce transaction costs.

In many ways, the trusted third-party model continues to work well.[113] As a result, there are some cryptocurrencies that actually trade ownership off the chain, relying on the intermediary to legitimize the transaction.[114]

---

109. *See generally* U.S. DEP'T OF JUST., CRYPTOCURRENCY ENFORCEMENT FRAMEWORK (2020), https://www.justice.gov/cryptoreport [https://perma.cc/74A4-RM46].

110. Hossein Nabilou & André Prüm, *Central Banks and Regulation of Cryptocurrencies*, 39 REV. BANKING & FIN. L. 1003, 1005 (2020).

111. SATOSHI NAKAMOTO, BITCOIN: A PEER-TO-PEER ELECTRONIC CASH SYSTEM 1 (2008).

112. Erik Feyen, Jon Frost, Leonardo Gambacorta, Harish Natarajan & Matthew Saal, *Fintech and the Digital Transformation of Financial Services: Implications for Market Structure and Public Policy*, BANK FOR INT'L SETTLEMENTS PAPERS, July 2021, at 2 https://www.bis.org/publ/bppdf/bispap117.pdf [https://perma.cc/2ACX-998A] ("A fundamental feature of payment markets is the need to keep track of payment obligations, and to verify the identity of account holders or the veracity of payment tokens.") (citation omitted).

113. *See* Dirk A. Zetzsche, Douglas W. Arner & Ross P. Buckley, *Decentralized Finance*, 6 J. FIN. REG. 172, 191 (2020), https://doi.org/10.1093/jfr/fjaa010 [https://perma.cc/7HG4-NZKX] (highlighting that the current financial system is built to address compliance obligations).

114. *See* Sarah Jane Hughes & Stephen T. Middlebrook, *Advancing A Framework for Regulating Cryptocurrency Payments Intermediaries*, 32 YALE J. ON REG. 495, 497–98 (2015).

> A growing percentage of transactions, however, take place through one or more intermediaries. Intermediaries act as custodians of cryptocurrency or cryptocurrency credentials originally belonging to their clients and may facilitate and clear transactions for clients without updating the public ledger. Such transactions are referred to as taking place "off the block chain." Off the block chain transactions may not appear in the public ledger at all, or, if they do, they appear as transactions involving not the sender and receiver, but the

Understanding the regulatory model for cryptocurrency transactions and transactions of nonfungible digital assets, therefore, will depend on the nature of the particular transaction. Some transactions will be for fungible cryptocurrency tokens, such as Bitcoin or Ether (Eth), that are written directly to the distributed ledger.[115] Other transactions for fungible tokens will be noted by the trusted third-party intermediary in the intermediary's own ledgers to reduce the transaction costs associated with changes to the distributed ledger.[116] And other transactions will be for nonfungible tokens, some of which will be on chain and others will be noted by trusted intermediaries and recorded off chain.[117]

Blockchain technology provides a great solution to the potential for double-spending, or having two parties make simultaneous claims to the funds while they are in transit.[118] Placing the record of the transaction into the distributed ledger assures that the same token cannot be used more than once.[119] But this is just one of many issues for financial transactions. Additional risks include "concerns about fraud, market manipulation, financial crime, consumer protection, liability issues in distributed ledgers, the development of large,

---

intermediaries.

Id.

115. *See* Ryan Haar, *Ethereum: What You Should Know Before You Invest*, NEXTADVISOR (May 3, 2022), https://time.com/nextadvisor/investing/cryptocurrency/what-is-ethereum/ [https://perma.cc/HJZ2-QNG5] ("Ethereum is a software platform that runs on a blockchain. Users can interact with the platform using ether, the cryptocurrency associated with Ethereum—or buy and hold it as a store of value. Ethereum is commonly used by developers, but there are people who also invest in the crypto for its potential to be worth more over time.").

116. Nathan Reiff, *Blockchain Won't Cut Out Intermediaries After All*, INVESTOPEDIA (Oct. 27, 2021), https://www.investopedia.com/tech/blockchain-wont-cut-out-intermediaries-after-all/ [https://perma.cc/XQG2-SMMB].

117. *On-chain NFTs and Why They're Better*, ART HAUS, https://art.haus/on-chain-nfts-and whytheyrebetter/#:~:text=One%20crucial%20difference%20between%20on,location%20of%20the%20digital%20art [https://perma.cc/NBS3-ERLZ].

118. Nabilou & Prüm, *supra* note 110, at 1005–06; *see also What Is Double-Spending?*, CRYPTOPEDIA (June 24, 2021), https://www.gemini.com/cryptopedia/double-spending-problem-crypto [https://perma.cc/GW7D-ARQD].

> Double-spending is simply the process of making two payments with the same currency or funds in order to deceive the recipient of those funds. With physical currency, this really isn't possible. You can't give two people the same $20 bill or silver coin. With most online payments, you trust a third party to make sure funds are sent and received properly. Banks, credit card companies, and payment processors validate the transactions themselves and minimize the risk of double-spending. With cryptocurrency, however, there's no third-party intermediary—just the sender and the recipient. How can crypto holders protect themselves against double-spending? The answer is on the blockchain.

Id.

119. CRYPTOPEDIA, *supra* note 118.

closed networks that can potentially create barriers to entry, data protection, taxation policy for cryptocurrencies, monetary policy, and financial stability."[120]

Given this long list of potential issues, it is not surprising that each of the U.S. financial regulatory bodies is seeking to be part of the regulatory solution.[121] There are four key regulatory regimes:

> [1] Financial Crimes Enforcement Network (FinCEN): Regulates all crypto assets for [anti-money laundering (AML) and combating the financing of terrorism (CFT)] purposes.[122]
>
> [2] US Securities and Exchange Commission (SEC): Regulates crypto assets considered securities by applying the *Howey* test.[123]
>
> [3] Commodity Futures Trading Commission (CFTC): Regulates virtual currencies which are considered commodities (Bitcoin and Ethereum).[124]
>
> [4] Officer of the Comptroller of Currency (OCC): For banks participating in the crypto ecosystem.[125]

In 2021, the Financial Action Task Force (FATF) updated guidance provided by the various regulatory agencies with an effort to emphasize the

---

120. Nabilou & Prüm, *supra* note 110, at 1007–08 (internal citations omitted).

121. Brennan, McDougall, Hornung, Litwack & Zuberi, *supra* note 108.

> State regulators apply state money transfers laws. The IRS considers cryptocurrency property and subject to capital gains tax. The CFTC considers cryptocurrency to be a commodity and subject to trading regulations. The SEC suggests that cryptocurrencies are securities. The U.S. Treasury, via the Financial Crimes Enforcement Network (FinCEN), considers it a currency subject to Office of Foreign Asset Control (OFAC) sanctions.

Id.

122. *See Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT)*, INT'L MONETARY FUND, https://www.imf.org/external/np/leg/amlcft/eng/ (last visited Nov. 18, 2022) ("Money laundering and the financing of terrorism are financial crimes with economic effects. Money laundering requires an underlying, primary, profit-making crime (such as corruption, drug trafficking, market manipulation, fraud, tax evasion), along with the intent to conceal the proceeds of the crime or to further the criminal enterprise.").

123. Paul Kim, *The* Howey *Test: A Set of Rules That Determine if an Investment is a Security*, Bus. INSIDER (May 31, 2022), https://www.businessinsider.com/personal-finance/howey-test#:~:text=The%20Howey%20test%20determines%20if,from%20the%20efforts%20of%20others [https://perma.cc/R8UJ-23BJ].

124. *Customer Advisory: Understand the Risks of Virtual Currency Trading*, CFTC, https://www.cftc.gov/LearnAndProtect/AdvisoriesAndArticles/understand_risks_of_virtual_currency.html [https://perma.cc/3YGM-WQ2V].

125. *Crypto Travel Rule in United States by FinCEN*, NOTABENE , https://notabene.id/world/usa [https://perma.cc/LN22-79WT] ("[W]here [the Financial Action Task Force (FATF)] uses 'virtual assets' and 'VASPs,' FinCEN's guidance uses money services businesses (MSBs.) and convertible virtual currencies (CVCs).").

risk-based approach to cryptocurrency transactions, the emergence of NFTs, and the expanded threats of ransomware.[126] In 2021, for FinCEN raised concerns that the most pressing concern has been the growth of cryptocurrency-fueled ransomware attacks.[127]

As a result of these concerns, FinCEN continues to require anti-money laundering protocols and know your customer (KYC) banking regulations for most cryptocurrency transactions, which will likely include all forms of tokens, unless the asset is not merely nonfungible but also truly non-tradable.[128] After all, just because each digital object has a unique serial number, that does not transform the object from a commodity into a unique asset. Automobiles have vehicle identification numbers making each automobile unique, but in the aggregate, there is a robust market for largely interchangeable vehicles available for sale, lease, and trade. Each bill of paper currency has a unique serial number, but the currencies remain wholly fungible.

Commodities can be tokenized using NFTs, but that does not mean there are not markets for those items subject to financial disclosure regulations. "In 2011, FinCEN issued a final rule that, among other things, defined 'money transmission services' to include accepting and transmitting 'currency, funds, or other value that substitutes for currency by any means.' "[129] The use of the phrase "other value that substitutes for currency" provided a broad,

126. U.S. DEP'T OF THE TREASURY FIN. ACTION TASK FORCE, DRAFT UPDATED GUIDANCE FOR A RISK-BASED APPROACH TO VIRTUAL ASSETS AND VASPS 4 (2021), https://www.fatf-gafi.org/media/fatf/documents/recommendations/March%202021%20-%20VA%20Guidance%20update%20-%20Sixth%20draft%20-%20Public%20consultation.pdf [https://perma.cc/F8Q2-MKAH].

127. *See* U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, FINCEN ADVISORY FIN-2021-A004, ADVISORY ON RANSOMWARE AND THE USE OF THE FINANCIAL SYSTEM TO FACILITATE RANSOM PAYMENTS 4, 7 (2021), https://www.fincen.gov [https://perma.cc/P6LB-DKA5] ("The severity and sophistication of ransomware attacks continue to rise across various sectors, particularly across governmental entities, and financial, educational, and healthcare institutions. . . . FinCEN's review of BSA data has identified DarkSide and Sodinokibi/REvil as among the most costly ransomware variants in the first six months of 2021. During this timeframe, 458 ransomware related transactions were reported with a total value of $590 million.").

128. *See* U.S. DEP'T OF JUST., *supra* note 109, at 22, 39, 41 ("In the United States, individuals and entities that offer money transmitting services involving virtual assets, such as cryptocurrency exchanges and kiosks, as well as certain issuers, exchangers, and brokers of virtual assets, are considered [money services businesses (MSBs)].").

129. *Id.* at 24; *see also* Bank Secrecy Act Regulations; Definitions and Other Regulations Relating to Money Services Businesses, 76 Fed. Reg. 43585, 43596 (July 21, 2011) (to be codified at 31 C.F.R. pts. 1010, 1021, 1022); 31 C.F.R. § 1010.100(ff)(5)(i)(A) (2021).

transactional approach to value storage and various substitutes for traditional fungible assets.[130]

For virtual worlds involving cryptocurrencies and tradable NFTs,[131] FinCEN has consistently demanded that anyone who trades in these tokens will be required to register, to file Suspicious Activity Reports (SARs), and to comply with anti-money laundering requirements.[132] As a result, the numerous KYC and other banking requirements suggest that most tokens might be better characterized and regulated as securities, which may actually prove more flexible to the enterprises trading the assets.

The DAO organizational structure is particularly inimical to the KYC and AML obligations. "These reporting requirements are incredibly expensive and are difficult for 'traditional' companies to comply with. Considering the fact that most DAO members are basically anonymous, the AML/KYC requirements alone would be prohibitive."[133] A DAO of any scale would require some form of centralized reporting obligations that would undermine the anonymity, flexibility, and shared governance of the DAO ethos. But both DAOs and more traditional entities may actually find benefits within the umbrella of traditional securities law rather than banking regulations.

ii. DAOs and the Potential Disclosure Requirements of the Corporate Transparency Act

In 2021, Congress created another law designed to protect markets and investments from opaque financial services. The Corporate Transparency Act (CTA) was adopted as an amendment to the Anti-Money Laundering Act of

130. *See* Financial Crimes Enforcement Network; Amendment to the Bank Secrecy Act Regulations-Definitions and Other Regulations Relating to Money Services Businesses, 74 Fed. Reg. 22129, 22137 (May 12, 2009) (to be codified at 31 C.F.R. pt. 103); U.S. DEP'T OF JUST., *supra* note 109, at 24.

131. *See* U.S. DEP'T OF JUST., *supra* note 109 at 56 ("A non-convertible virtual currency may effectively become a convertible virtual currency where a robust unofficial secondary market for the currency develops and provides the opportunity to exchange the 'non-convertible' currency for fiat or other virtual currency."); FINANCIAL ACTION TASK FORCE, VIRTUAL CURRENCIES: KEY DEFINITIONS AND POTENTIAL AML/CFT RISKS 4 (2014), http://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf [https://perma.cc/3QWU-D7DU].

132. *See* U.S. DEP'T OF THE TREASURY FIN. CRIMES ENF'T NETWORK, , FINCEN GUIDANCE FIN-2013-G001, APPLICATION OF FINCEN'S REGULATIONS TO PERSONS ADMINISTERING, EXCHANGING, OR USING VIRTUAL CURRENCIES (2013), https://www.fincen.gov/sites/default/files/shared/FIN-2013-G001.pdf [https://perma.cc/F4YD-AKXQ].

133. Rodman, *supra* note 81.

2020.[134] The law was developed to help combat money laundering, and is primarily focused on the use of shell companies.[135] "The CTA, part of the Anti-Money Laundering Act of 2020, established beneficial ownership information reporting requirements for certain types of corporations, limited liability companies, and other similar entities created in or registered to do business in the United States."[136]

Proposed regulations focus on entities filed through a state's secretary of state office, including corporations, LLCs, and limited liability partnerships. "Under the proposed rules, a domestic reporting company is any entity that is a corporation, a limited liability company, or other entity that is created by the filing of a document with a secretary of state or similar office of a U.S. jurisdiction."[137] While broad in scope, the CTA and the initial regulation's focus on formation through a document filed with the secretary of state may create at least a short-term opportunity for DAO proponents to promote the use of DAOs as an opportunity to avoid CTA reporting obligations.[138] Invariably, however, this distinction will eventually be addressed by regulation or statute.

iii. Securities Regulation

Although the operations of FinCEN are based on highly specific statutes, the Securities and Exchange Commission (SEC) has very broad statutory authority, and it will continue to expand its role in the metaverse and Web3 financing.

The SEC will continue to play a significant role in regulating the unregistered sale of tokens and digital assets that have the attributes of

---

134. Corporate Transparency Act (CTA), Pub. L. No. 116-283, 134 Stat. 4547 (codified in scattered sections of 31 U.S.C.); *see* Brian K. Prosek, John R. Chadd & Kalynn G. Walls, *The Corporate Transparency Act*, NAT. L. REV. (Dec. 1, 2021), https://www.natlawreview.com/article/corporate-transparency-act [https://perma.cc/6RWT-PH9C].

135. *See* Brooke Tansill, *The Corporate Transparency Act: What Practitioners Need To Know*, VA. LAW., June 2021, at 14–15 https://virginialawyer.vsb.org/publication/?i=708504&article_id=4039086&view=articleBrowser&ver=html5 [https://perma.cc/3837-LD9R].

136. Press Release, Fin. Crimes Enf't Network, FinCEN Issues Proposed Rule for Beneficial Ownership Reporting to Counter Illicit Finance and Increase Transparency (Dec. 7, 2021), https://www.fincen.gov/news/news-releases/fincen-issues-proposed-rule-beneficial-ownership-reporting-counter-illicit [https://perma.cc/7RCP-HSBA].

137. Thomas G. Appleman, Vera S. Hansen, & Arthur L. Griem, *FinCEN Publishes Notice of Proposed Rulemaking on the Corporate Transparency Act*, NAT. L. REV. (Dec. 21, 2021), https://www.natlawreview.com/article/fincen-publishes-notice-proposed-rulemaking-corporate-transparency-act [https://perma.cc/V7Z4-9T64].

138. Nick Oberheiden, *5 Things to Consider When Creating a DAO*, JD SUPRA (Feb. 8, 2022), https://www.jdsupra.com/legalnews/5-things-to-consider-when-creating-a-dao-5888423/ [https://perma.cc/8ZTK-SLTQ] ("As unincorporated entities, [DAOs] do not need to follow the legal formalities of incorporation such as registration. . . .").

securities. Any collaboration by participants within the virtual world to monetize the digital assets created within the platform will trigger securities regulation when the activities are collaborative, but the value is not created by the effort of the individual users.[139] State blue sky laws may play a role in protecting the public from unscrupulous in-world get rich quick schemes, but only to the extent there is state jurisdiction over the activity.[140] For DAOs, the theoretical argument is that the collective ownership and shared community responsibility suggests that value is created by the actions of each individual.[141] But this may not be the reality for all DAOs, particularly if tokens derived from payment carry less per-unit value than tokens derived from effort. The SEC and state regulators could potentially treat many of the DAO structures as securities notwithstanding the lack of a central manager directing the enterprise while theDAO token owner sits back to make profit on the investment in a DAO token.[142]

The Supreme Court has explained that a security includes many different certificates denominating ownership. "Congress' purpose in enacting the securities laws was to regulate *investments*, in whatever form they are made and

---

139. SEC v. W.J. Howey Co., 328 U.S. 293, 298–99 (1946) ("[A]n investment contract for purposes of the Securities Act means a contract, transaction or scheme whereby a person invests his money in a common enterprise and is led to expect profits solely from the efforts of the promoter or a third party . . . .").

140. Mark Astarita, *Blue Sky Law*, SEC L. (Dec. 5, 2019), https://www.seclaw.com/glossary/blue-sky-law/ [https://perma.cc/Y8KR-KRR8] ("A blue sky law is a state law regulating the offer and sale of securities, as well as the regulation of broker dealers and stock brokers.").

141. The SEC has rejected this position. *See* Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Exchange Act Release No. 81207 4 (July 25, 2017), http://www.sec.gov/litigation/investreport/34-81207.pdf [https://perma.cc/7NAN-DYHQ] (hereinafter SEC DAO REPORT).

142. *See* 15 U.S.C.A. § 77b(a)(1).

> The term "security" means any note, stock, treasury stock, security future, security-based swap, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security, certificate of deposit, or group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guarantee of, or warrant or right to subscribe to or purchase, any of the foregoing.

Id. A particular DAO NFT may fall into the definition of many of these certificates separate from any attributes that make it an investment contract.

by whatever name they are called."[143] In *SEC v. W.J. Howey Co.*,[144] the Court offered the definition of an investment contract as "whether the scheme involves an investment of money in a common enterprise with profits to come solely from the efforts of others."[145] In *SEC v. Edwards*,[146] the Court further explained that "when we held that 'profits' must 'come solely from the efforts of others,' we were speaking of the profits that investors seek on their investment, not the profits of the scheme in which they invest."[147] A DAO that will grow in value primarily through its popularity and size may well have increased value of investment or dividends potentially making the token regulable as an investment contract, notwithstanding the direct management provided in the DAO to every token holder.[148]

A suggestion has been floated that a DAO operated as a general partnership should be immune from securities laws because, essentially, the risk one assumes as a general partner should make one an active participant in the investment.[149] The caselaw, however, is more nuanced, suggesting that in practice most general partners are active participants.[150] To the extent that the general partnership is comprised of limited partnerships or other passive, pass-through entities, the factual assertion of active management would disappear and the "efforts of others" analysis would likely result in these entities also operating as investment contracts.

The SEC has taken a similar approach. Reviewing the first DAO initial coin offering (ICO), the SEC largely looked past the formalities of DAO shared governance to find that the overall structure forced the investors to rely on the organizers' unique positions of knowledge, skill, and control to create value in the tokens.[151] As such, the tokens were securities. "The voting rights afforded DAO Token holders did not provide them with meaningful control over the enterprise, because (1) DAO Token holders' ability to vote for contracts was a

143. Reves v. Ernst & Young, 494 U.S. 56, 61 (1990); s*ee also* 15 U.S.C.A. § 77b(a)(1).

144. 328 U.S. 293 (1946).

145. *Id*. at 301.

146. 540 U.S. 389 (2004).

147. *Id.* at 393–94.

148. SEC DAO REPORT, *supra* note 141, at 4, 12–14.

149. *See* Rodman, *supra* note 81.

150. *See* SEC v. Merchant Capital, LLC, 483 F.3d 747, 755 (11th Cir. 2007) ("A general partnership interest is presumed not to be an investment contract because a general partner typically takes an active part in managing the business and therefore does not rely solely on the efforts of others."); SEC v. Schooler, 902 F. Supp. 2d 1341, 1346 (S.D. Cal. 2012).

151. SEC DAO REPORT, *supra* note 141, at 12–14 ("Even if an investor's efforts help to make an enterprise profitable, those efforts do not necessarily equate with a promoter's significant managerial efforts or control over the enterprise.").

largely perfunctory one; and (2) DAO Token holders were widely dispersed and limited in their ability to communicate with one another."[152]

The characteristics that will determine these outcomes will be based in the intersection between the DAO's governance documents, its end user license agreement, and the smart contract provisions embedded into the NFTs. As a result, the programming choices that define the smart contract provisions may define whether or not the NFT adopted by a particular DAO will be regulated as an investment contract.

iv. Foreign Investment Regulation

If the predictions of the metaverse prove to be even partially correct, then the metaverse will have the potential to disrupt the institutions and relations that govern both domestic and international politics. No country is more concerned about that disruption than China, which tightly controls all means of dissent and is increasingly focused on all forms of international commerce.[153] Russia and

---

152. *Id.* at 14.

153. *See* Drake Bennett, *The Metaverse Gives China a New Digital Playground to Censor*, BLOOMBERG (Dec. 10, 2021), https://www.bloomberg.com/news/newsletters/2021-12-10/china-metaverse-offers-new-digital-playground-for-censorship [https://perma.cc/FLV2-KXDY].

> China's reticent approach to gaming, accompanied by encouragement for young people to go out and partake in real-world sports, is perhaps a preview of its view of the metaverse. . . .
>
> In one corner would be the authoritarians eager to limit the metaverse, or perhaps even to use it as a pretext for expanding existing prohibitions. The always-on nature of the imagined virtual world, its blurred boundary with so-called meatspace, could represent possible new frontiers of surveillance and restrictions. Robert Williams, a China policy researcher at Yale Law School, points out in an email that the definition of what now constitutes problematic online gaming could end up broadening "in a social context where the lines between physical and digital reality are somewhat blurred."

Id.; *see also China Targets Online Platforms in Quest to 'Clean Up' Internet*, YAHOO! NEWS (Dec. 23, 2021), https://news.yahoo.com/china-targets-online-platforms-quest-113410595.html [https://perma.cc/Y3K2-3JZZ] ("China will scrutinise online platforms . . . as part of its drive to 'clean up' the internet . . . . The investigation comes against the backdrop of a wide-ranging crackdown by regulators on several sectors, with officials tightening oversight of companies in technology, real estate, gaming, education, cryptocurrencies and finance."); Alex Chan, *Hong Kong Pro-Democracy News Site Closes After Raid, Arrests*, NPR (Dec. 29, 2021), https://www.npr.org/2021/12/29/1068696336/hong-kong-police-raid-pro-democracy-news-outlet-arrest-6 [https://perma.cc/E3DS-26HV]; OFF. OF THE U.S. SEC'Y OF STATE, THE ELEMENTS OF THE CHINA CHALLENGE 28, 30 (2020) https://www.state.gov/wp-content/uploads/2020/11/20-02832-Elements-of-China-Challenge-508.pdf [https://perma.cc/5KXR-L7W3] ("China's pursuit of global preeminence and drive to remake world order flow from the CCP's overarching sensibility. That sensibility is authoritarian, collectivist, and imperial. . . . [I]t promulgates among the people a rigid ideology from which it tolerates no dissent."); THE LONGER TELEGRAM: TOWARD A NEW AMERICAN CHINA STRATEGY 48–49 (2021) https://www.atlanticcouncil.org/wp-content/uploads/2021/01/The-

other foreign governments have their own agendas regarding U.S. technology, and those programs may extend into the work in artificial intelligence, communications technology, 5G, synthetic media, NFTs, cryptocurrencies and blockchain services, and other innovations that will fuel Web3 growth and the proliferation of the metaverse.[154] The U.S. government, in contrast, is very concerned that foreign control of these technologies would have the potential to give foreign adversaries an advantage over the U.S. and its strategic agenda, and could be used to harm either the U.S. domestic agenda or be used to compete unfairly on an economic basis with U.S. companies.[155]

To address these concerns, in 2018, Congress passed the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).[156] The purpose of the law was to expand the jurisdiction of the Committee on Foreign Investment in the United States (CFIUS).[157] CFIUS has operated since 1975, granting the President authority "to block or suspend proposed or pending foreign 'mergers, acquisitions, or takeovers' of U.S. entities, including through joint ventures, that threaten to impair the national security."[158] Implementing

---

Longer-Telegram-Toward-A-New-American-China-Strategy.pdf [https://perma.cc/2TDY-JMR2**]** ("China will reject all forms of international human rights pressure concerning Xinjiang, Tibet, Hong Kong, as well as other forms of domestic political and religious dissent within China proper, as the regime doubles down through its repressive control systems in defense of the Leninist state.").

154. *See, e.g.*, Anna Baydakova, *Russian Government Introduces Crypto Bill to Parliament Over Central Bank Objections*, COINDESK (Feb. 21, 2022), https://www.coindesk.com/policy/2022/02/21/russian-government-introduces-crypto-bill-to-parliament-over-central-bank-objections/ [https://perma.cc/5S3A-EVAJ]; *see also* Alun John, Samuel Shen & Tom Wilson, *China's Top Regulators Ban Crypto Trading and Mining, Sending Bitcoin Tumbling*, REUTERS (Sep. 24, 2021), https://www.reuters.com/world/china/china-central-bank-vows-crackdown-cryptocurrency-trading-2021-09-24/ [https://perma.cc/TD7C-YBTB].

155. Ryan Browne, *Biden Just Put Out an Executive Order on Cryptocurrencies—Here's Everything That's in it*, CNBC (Mar. 9, 2022), https://www.cnbc.com/2022/03/09/heres-whats-in-bidens-executive-order-on-crypto.html [https://perma.cc/UU8Q-KM2W]; Tami Stark & Ben Elron, *US Regulators Seek to Prevent Use of Crypto to Circumvent Russia Sanctions*, WHITE & CASE (Apr. 6, 2022), https://www.whitecase.com/insight-alert/us-regulators-seek-prevent-use-crypto-circumvent-russia-sanctions [https://perma.cc/3MUD-RT3U].

156. Foreign Investment Risk Review Modernization Act of 2018, Pub. L. No. 115-232, 132 Stat. 2173 (2018).

157. *See* Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. 3112, 3112 (Jan. 17, 2020) (to be codified at 31 C.F.R. pts. 800, 801) ("FIRRMA amended and updated section 721 (section 721) of the Defense Production Act of 1950 (DPA), which delineates the authorities and jurisdiction of the Committee on Foreign Investment in the United States (CFIUS or the Committee).").

158. JAMES K. JACKSON & CATHLEEN D. CIMINO-ISAACS, CONG. RSCH. SERV., IF10952, CFIUS Reform Under FIRRMA 1 (2020), https://sgp.fas.org/crs/natsec/IF10952.pdf [https://perma.cc/W639-WSYD] ("CFIUS is an interagency body comprised of nine Cabinet members, two ex officio members, and others as appointed that assists the President in overseeing the national security risks of FDI in the U.S. economy.").

regulations promulgated by the U.S. Department of Treasury (which serves as chair of CFIUS) took effect in February 2020 which expanded the scope of CFIUS review, making the process potentially relevant to many of the global transactions that could fund or shape the metaverse. The regulations address the expansion of CFIUS review of "TID U.S. businesses," a new acronym for critical technologies, critical infrastructure, and personal data.[159] This includes transactions that provide foreign investors access to material nonpublic technical information, sensitive personal data, and "substantive involvement in the U.S. business's decision-making with respect to the technology, infrastructure, or data."[160]

Specifically, the final regulations include, among other reasons for review, transactions involving:

> (3) Any involvement, other than through voting of shares, in substantive decisionmaking of the TID U.S. business regarding:
> (i) The use, development, acquisition, safekeeping, or release of sensitive personal data of U.S. citizens maintained or collected by the TID U.S. business;
> (ii) The use, development, acquisition, or release of critical technologies; or
> (iii) The management, operation, manufacture, or supply of covered investment critical infrastructure.[161]

The regulations also provide a lengthy definition of sensitive personal data that covers U.S. government and military personnel or contractors, financial data, health care and health status data, geolocation data, biometric and genetic data, stored communications, and more.[162] The scope of the sensitive personal data is sufficiently broad to include essentially all metaverse platform operators as well as most social media services. The only limitation is that the regulation excludes entities that have collected data on one million or fewer individuals, though this limitation will not apply if the entity has the capability to exceed the one-million individual threshold.[163]

---

159. *See* Antonia I. Tzinova, *New CFIUS Regulations Finally Take Effect*, HOLLAND & KNIGHT (Feb. 13, 2020), https://www.hklaw.com/en/insights/publications/2020/02/new-cfius-regulations-finally-take-effect [https://perma.cc/AR6E-SWYC]; Nicholas J. Spiliotes, Charles L. Capito & Joseph A. Benkert, *Foreign Investment 2020 (Part 3): CFIUS Spotlight on "TID" U.S. Businesses*, MORRISON & FOERSTER (Oct. 15, 2019), https://www.mofo.com/resources/insights/191015-foreign-investment-2020.html [https://perma.cc/U6MA-MGF8].

160. Tzinova, *supra* note 159.

161. Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. at 3127 (to be codified at 31 C.F.R. § 800.211(b)(3)).

162. *See id.* at 3132 (to be codified at 31 C.F.R. § 800.241(a)(1)(ii)).

163. *Id.* (to be codified at 31 C.F.R. § 800.241(a)(1)(i)(B)).

In addition to the inclusion of sensitive personal data, Congress extended FIRRMA's definition of " 'critical technologies' to include 'emerging and foundational technologies' controlled by the 2018 Export Control Reform Act (ECRA)."[164] This further extends the regulatory protection of Web3 under CFIUS.

The role of CFIUS in the metaverse is not hypothetical. In 2019, the Trump administration began a very public review of TikTok, threatening to ban the company because of its Chinese ownership.[165] Some of those actions were eventually reversed by the Biden administration, but additional reviews of Chinese investments were put in place, including many that will still impact Web3 and metaverse technologies.[166] The ownership of TikTok, in particular, was complicated because the Trump administration ordered both a CFIUS review and a separate executive order under "the International Emergency Economic Powers Act (IEEPA) to outright ban 'transactions' with entire companies."[167] The executive order was reversed by the subsequent Biden executive order,[168] while the CFIUS review of ByteDance's ownership of TikTok remains ongoing but in seeming abeyance.[169]

The role of CFIUS in TikTok is even more confounding since ByteDance did not acquire a U.S. company to obtain the sensitive personal data potentially

---

164. Adam Chan, *CFIUS, Team Telecom and China*, LAWFARE (Sept. 28, 2021), https://www.lawfareblog.com/cfius-team-telecom-and-china [https://perma.cc/T72A-U3DC]; *see also* Provisions Pertaining to Certain Investments in the United States by Foreign Persons, 85 Fed. Reg. at 3128 (to be codified at 31 C.F.R. § 800.215).

165. *See* Christopher M. Caparelli, *Taking on TikTok: CFIUS on the Front Page (and in the Fine Print)*, TORYS (Sept. 20, 2020), https://www.torys.com/our-latest-thinking/publications/2020/09/taking-on-tiktok [https://perma.cc/FX9X-VEVH] ("Shortly before the Trump administration's bans against TikTok and WeChat were set to take effect on September 20, two U.S. federal judges issued preliminary injunctions . . . . In the TikTok case, the court enjoined the government's ban on downloads and software updates of the popular application."); Emily Birnbaum, *"This Has Been Botched": This is What Makes Trump's TikTok Tirade so Unusual*, PROTOCOL (Aug. 6, 2020), https://www.protocol.com/cfius-tiktok-not-how-this-works [https://perma.cc/6Y6S-BHXU].

166. *See* Nova J. Daly, Nazak Nikakhtar, Daniel P. Brooks, John Allen Riggins & Adam M. Teslik, *Biden Administration Revokes Trump EOs Targeting TikTok, WeChat, and Other Chinese Software Apps; Initiates Broader Investigations into Software Apps by Foreign Adversaries*, WILEY (June 11, 2021), https://www.wiley.law/alert-Biden-Administration-Revokes-Trump-EOs-Targeting-TikTok-WeChat-and-Other-Chinese-Software-Apps-Initiates-Broader-Investigations-into-Software-Apps-by-Foreign-Adversaries [https://perma.cc/R8FP-3CNW].

167. *See* Chan, *supra* note 164.

168. *See* Daly, Nikakhtar, Brooks, Riggins & Teslik, *supra* note 166.

169. Rick Sofield, John Satira & Olivia Hinerfield, *TikTok and Oracle Ink Data-Storage Agreement in Apparent Effort to Avoid Further CFIUS Scrutiny*, VINSON & ELKINS (June 24, 2022), https://www.velaw.com/insights/tiktok-and-oracle-ink-data-storage-agreement-in-apparent-effort-to-avoid-further-cfius-scrutiny/ [https://perma.cc/2UYJ-GJTK].

held by TikTok.[170] Instead, it simply made its own application available in the U.S. using the Google Play Store and Apple App Store.[171]

Nonetheless, the lesson from TikTok and the expanded authority under FIRRMA will have a profound impact on the growth of Web3 and the metaverse. Foreign investments are being discouraged and regulatory scrutiny is expanding.

C. Privacy, Cybersecurity, and Additional Areas of Focus for Regulators

The metaverse will likely become home to many online pastimes beyond role-playing games and fantasy sports leagues. Among them will be those associated with public vice. These will include gambling, sales of drugs and illicit items, and pornographic adult entertainment. Some of these unsavory activities are more heavily regulated than others, and it is likely that the state and federal regulators of such activities will seek to regulate these activities. Financial services companies will not provide financial services for illegal activities and tend to avoid those companies which may trigger such regulatory scrutiny. Uses such as these could make collaborations by the financial services sector more difficult. However, it is also possible that the lure of the metaverse payday will encourage the financial sector to look beyond the sector of illegal activity in order to be part of the broader transition. Concerns over illegal activities might also drive corporations to segment and separate their operations, creating an internet of virtual worlds rather than a unified metaverse. Interoperable virtual worlds would help more risk-averse enterprises participate without taking on all the challenges of an unregulated, virtual wild west.

At the other end of the use case, to the extent the metaverse becomes a platform for online business meetings, trainings, and classroom settings, the platforms and the business operating on those platforms will also be required to comply with various Americans with Disabilities Act accommodation obligations for those consumers who have a medical impairment or health issue.[172] The structure of the metaverse must take into account the needs of those users who are hearing impaired, visually impaired, have motor-skill limitations, or have other special needs.[173] To the extent the metaverse is

170. *See* Daly, Nikakhtar, Brooks, Riggins & Teslik, *supra* note 166.

171. Elizabeth Atkin, *A Complete History of TikTok—From Launch and Banning Controversy, to Best Viral Trends*, METRO (Feb. 13, 2021), https://metro.co.uk/2021/01/01/a-complete-history-of-tiktok-launch-us-ban-and-best-viral-dances-13823263/ [https://perma.cc/3VZT-PVMD].

172. Squire Patton Boggs, *Employment Law In The Metaverse—Part 2*, FAMILY WEALTH REP. (Aug. 18, 2022), https://www.familywealthreport.com/article.php?id=195325#.YwuTj3bMKM8 [https://perma.cc/9NRA-LFPT].

173. *Id.*

offering an alternative to a public accommodation, the provider of that service must take reasonable steps to assure that all customers are able to take advantage of that service.[174]

This last set of obligations, in turn, requires the providers of the metaverse platform to address the social responsibility, as well as legal responsibility, it will have in managing the character and tone of the metaverse environment. Through enforcement of the terms of service, congressional adjustments to the Communications Decency Act § 230 safe harbor,[175] and updated privacy laws,[176] the success or failure of the metaverse may well depend on the extent to which privacy rights are protected and harmful, trolling behavior is curtailed. Like enterprises on the current internet, each service provider will have ongoing obligations to protect the privacy and security of the information and data of its customers as well, making compliance with applicable privacy and security laws an essential component of each company's metaverse strategy.[177]

Another of the significant risks lurking in a ubiquitous metaverse is the threat of cybersecurity breaches. Corporate espionage, ransomware attacks, international cyberwarfare incursions, and old-fashioned hacking will all move

---

174. *Id.*

175. *See* 47 U.S.C § 230; George Fishback, *How the Wolf of Wall Street Shaped the Internet: A Review of Section 230 of the Communications Decency Act*, 28 TEX. INTELL. PROP. L.J. 275, 283–90 (2020); Jon M. Garon, *Constitutional Limits on Administrative Agencies in Cyberspace*, 8 BELMONT L. REV 499, 536 (2021).

176. *See* Rick Buck, *Introduction to Data Privacy in 2021*, WIREWHEEL (Oct. 28, 2021), https://wirewheel.io/data-privacy-laws-guide/ [https://perma.cc/Z7V9-6UNY] ("Over the past few years, the proliferation of data privacy laws has accelerated around the world. And this trend is not about to stop. According to Gartner, 'by 2023, 65% of the world's population will have its personal data covered under modern privacy regulations.' "); Cynthia J. Larose & Christopher J. Buontempo, *US State Privacy Law Update*, NAT. L. REV. (June 11, 2021), https://www.natlawreview.com/article/us-state-privacy-law-update-june-11-2021 [https://perma.cc/956L-AZWQ].

177. *See* Wayne Unger, *Reclaiming Our Right to Privacy by Holding Tech. Companies Accountable*, 27 RICH. J.L. & TECH. 1, 16–17 (2020) ("Privacy trade groups frame compliance with privacy and security laws as a means of reducing corporate risk—not a means of actually protecting individuals' PI by improving a business's privacy and security practices."); Stanley A. Marciniak III, Comment, *Too Big to Protect: A Dodd-Frank Framework for Protecting 21st Century American Consumer Privacy Rights*, 59 DUQ. L. REV. 329, 348–49 (2021) ("If Americans cannot stop 'pervasive' data collection, use, and sale, the question becomes: '[w]hat do we do?'. . . . In short, the answer lies in the law. Imposing accountability-based legal structures on corporations that define 'fair and unfair uses of information' can catalyze a solution." (quoting FRANK PASQUALE, THE BLACK BOX SOCIETY: THE SECRET ALGORITHMS THAT CONTROL MONEY AND INFORMATION 52 (2015)); Anita L. Allen, *An Ethical Duty to Protect One's Own Information Privacy?*, 64 ALA. L. REV. 845, 852 (2013) ("In addition to 'first-order' duties to protect one's own privacy, there may also be 'second-order,' derivative duties to protect one's own privacy for the sake of specific others or the community.").

to the metaverse because that's where the money is.[178] The FBI has identified theft in the cryptocurrency marketplace as one of the key concerns for the cryptocurrency industry.[179] Among the myriad of fears and threats, the FBI report notes that "criminals routinely infect victims' computers and servers with ransomware,"[180] others "demand payment after threatening to distribute confidential or embarrassing information (such as nude photos in cases of 'sextortion'),"[181] organize and fund terrorism,[182] traffic in child pornography,[183] counterfeit goods and services,[184] and commit tax fraud.[185]

In a 2016 survey of corporate boards at publicly traded corporations, 70% stated that cybersecurity was the top concern for their company.[186] "The organizations that rely on data have increasingly come to fear 'data breaches,' 'security incidents,' 'malicious actors,' 'ransomware' and a host of emerging threats that take up growing amounts of time in server rooms, boardrooms and, if recent trends continue, courtrooms."[187]

The responsibility for oversight to forestall these breaches, hacks, incursions, and exfiltrations will fall on the entities that comprise the metaverse, and the responsibility for acting responsibly will fall on the officers and directors of those enterprises. Corporations operate through their centralized

178. *See Willie Sutton*, FBI: HISTORY, https://www.fbi.gov/history/famous-cases/willie-sutton [https://perma.cc/R5XR-NPBY] (highlighting the gentlemen bank robber, known for his polite demeanor and dapper dress, who famously answered the question "why he robbed banks" by saying, "because that's where the money is.").

179. U.S. DEP'T OF JUST., *supra* note 109, at viii. ("[I]llicit uses of cryptocurrency typically fall into three categories: (1) financial transactions associated with the commission of crimes; (2) money laundering and the shielding of legitimate activity from tax, reporting, or other legal requirements; or (3) crimes, such as theft, directly implicating the cryptocurrency marketplace itself.").

180. *Id.* at 7.

181. *Id.*

182. *Id.* at 7, 11.

183. *Id.* at 10.

184. *Id.* at 12.

185. *Id.* at 14. In the first six months of 2019, data breaches compromised an estimated 4.1 billion records, 3.2 billion of which came from just eight isolated breaches. Davey Winder, *Data Breaches Expose 4.1 Billion Records in First Six Months of 2019*, FORBES (Aug. 20, 2019) https://www.forbes.com/sites/daveywinder/2019/08/20/data-breaches-expose-41-billion-records-in-first-six-months-of-2019/?sh=46f17810bd54 [https://perma.cc/3MK6-5XAB].

186. Charles Weinstein, *Concerns About Risks Confronting Boards – 2015 Survey*, EISNERAMPER (Mar. 2016), http://www.eisneramper.com/Risk-Management-Cybersecurity-Social-Media-0116.aspx [https://perma.cc/5LG6-RCRE].

187. Gerard M. Stegmaier & Courtney E. Fisher, *Caveat Director Analyzing Cybersecurity Challenges in Corporate Governance*, 38 DEL. LAW. 14, 14 (2020).

management, while DAOs operate through the community will.[188] The business judgment rule provides corporate directors a strong presumption against liability.

> The business judgment rule is an acknowledgment of the managerial prerogatives of Delaware directors . . . . It is a presumption that in making a business decision the directors of a corporation acted on an informed basis, in good faith and in the honest belief that the action taken was in the best interests of the company.[189]

Under the business judgment rule, decisions made by corporate directors are generally not subject to shareholder liability or other second-guessing provided they are made in good faith.[190] To achieve these protections, enterprises and the directors of enterprises need to undertake meaningful corporate compliance programs for each area in which there are affirmative regulations as well as in areas where there may be significant risk of loss or harm.[191]

> If, as many believe, cybersecurity incidents are inevitable, officers and directors will face an increasingly difficult challenge to respond systematically to these enterprise risks in ways that are demonstrable. Although the business judgment rule provides formidable protection, how business judgment is exercised and the defense of its exercise in the area of cybersecurity and its oversight is growing rapidly. The situation is more complicated because security is but one among many demands on the enterprise. . . . [W]hile companies could take a series of security precautions, directors must help ensure and provide guidance regarding all corporate interests among many potential stakeholders and with

188. Cathy Hackl, *What Are DAOs And Why You Should Pay Attention*, FORBES (June 1, 2021), http://forbes.com/sites/cathyhackl/2021/06/01/what-are-daos-and-why-you-should-pay-attention [https://perma.cc/2VZA-83EG] ("The governance of DAOs is based on community, while traditional companies' governance is mostly based on executives, Board of Directors, activist investors. etc. DAOs' operations are fully transparent and global, meanwhile, traditional companies' operations are private, only the organization know what is happening, and they are not always global.").

189. Aronson v. Lewis, 473 A.2d 805, 812 (Del. 1984) (first citing Zapata Corp. v. Maldonado, 430 A.2d 779, 782 (Del. 1981); then citing Kaplan v. Centex Corp., 284 A.2d 119, 124 (Del. Ch. 1971); and then citing Robinson v. Pittsburgh Oil Refin. Corp. 126 A. 46 (Del. Ch. 1924)), *overruled on other grounds by* Brehm v. Eisner, 746 A.2d 244, 264 (Del. 2000); *see* Steven A. Lauer & Joseph E. Murphy, *Compliance and Ethics Programs: What Lawyers Need to Know to Understand the Development of This Field*, 75 BUS. LAW. 2541, 2560 (2020).

190. Lauer & Murphy, *supra* note 189, at 2560.

191. *See id.* at 2561; *see also* Stegmaier & Fisher, *supra* note 187, at 23.

substantial personal risk.[192]

For DAOs, these protections may not be available. The lack of structured decision-making, the ability to inform oneself, and the other attributes of management will not be present. Suddenly, those features may become legal liabilities—bugs in the corporate code of conduct. Even for traditional corporations, the need to create robust privacy, cybersecurity, and legal compliance systems will be a time consuming and expensive task.

The challenges for operating in the fully realized metaverse are daunting, and it will likely emerge in fits and starts over many years. But as well the internet's transformation of media, gaming, commerce, and financial services, the potential for an immersive next stage in communications is anticipated too heavily for it to remain fiction. Someone will soon be willing this reality into existence. As such, the legal community must be ready to face what that reality will bring and help foster the best version of this next future.

V. TRANSACTING BUSINESS IN THE VIRTUAL WORLD

To focus the myriad of potential issues for the multiverse of evolving virtual worlds, this Article will use the fictional "Ginormaverse," a theoretical U.S.-based virtual world featuring many of the important aspects of a successful, commercially-focused, next-generation virtual world.[193] Ginormaverse provides services for work, education, entertainment, commerce, and news from its common platform. This Article is not using Ginormaverse because it discounts the potential of DAOs to help fuel a more disaggregated multiverse, but merely because it is reasonable to predict that the attributes of the metaverse will take on a homogenous state whether the ownership is highly distributed or highly concentrated.[194] The legal issues will be the same in both the ubiquitous metaverse and the fragmented multiverse; the difference will be a greater variety of contractual terms and compliance modalities.

These are some of the critical features of Ginormaverse:

- Each user has a verified identity, protected by an encryption technology, with multi-factor

192. Stegmaier & Fisher, *supra* note 187, at 23.

193. The name Ginormaverse was selected after a brief Internet search identified significant use for metaverse, ultraverse, megaverse, superverse, giantverse, gigantiaverse, universe, magaverse, whopperverse, and other names in the "verse" family. Whopperverse was not used but closely associated with both Burger King and Hershey's Whoppers Malted Milk Balls.

194. *See generally* Salvatore Ferraro, *What Limits Shareholder Activism is the Free-Rider Problem*, THE CONVERSATION (Dec. 11, 2019), https://theconversation.com/what-limits-shareholder-activism-is-the-free-rider-problem-127232 [https://perma.cc/R6GN-7KPD] ("Economists call it the free-rider problem. In essence it's the problem of individuals having little incentive to contribute to a collective resource when they can enjoy its benefits even if they don't.").

authentication. A user can operate within many of the worlds pseudonymously, but for non-entertainment purposes, most operations require a true identity.[195]

- Technology will allow users to shift from virtual reality to camera-based live images using augmented reality glasses or other means, so that a person's live image can be present within the virtual world when appropriate rather than just an avatar.
- Each user's avatars are portable, meaning that the avatars can be used with all their features, attributes, and digital property, across all other compatible platforms. There may be other universes that are not interoperable, but those become irrelevant outside the platform.
- Each category of commercial enterprise has a place in Ginormaverse. There are banks, retailers with home delivery, bookstores and libraries, offices, engineering labs, schools, social clubs, churches and similar houses of worship, conference centers, game rooms, and every other aspect of social interaction available in the United States. Existing major enterprises, including Microsoft, Amazon, and Google, will operate within the Ginormaverse environment as if the user were engaging with these providers directly through a computer or mobile device.

A. Terms of Service Agreements and the Law of the Metaverse

These policies, and many more, will be largely established by the Terms of Service Agreement (ToS) or End User License Agreement (EULA) provided by the platform and required as a condition of use by any person or enterprise wishing to interact within the virtual world.[196] Law365 explains that every software vendor requires an agreement to "limit [its] liability for damages"; "maintain control over distribution and use of . . . software"; "protect . . . rights to terminate licenses"; and "restrict abuses of software."[197] Other commentors

195. *See generally* Przemyslaw Palka, *The World of Fifty (Interoperable) Facebooks*, 51 SETON HALL L. REV. 1193, 1229–30 (2021) ("Put simply, products are interoperable if they can work together. . . . '[T]he ability to transfer and render useful data and other information across systems, applications, or components.' [John Palfrey & Urs Gasser] nuance the definition by distinguishing four layers of interoperability: technological, data, human, and institutional.") (quoting JOHN PALFREY & URS GASSER, INTEROP: THE PROMISE AND PERILS OF HIGHLY INTERCONNECTED SYSTEMS 5 (2012)).

196. *See*, *e.g.*, *Why Do You Need an End User License Agreement?*, LAW365 (Jan. 8, 2020), https://www.law365.co/blog/end-user-license-agreement [https://perma.cc/CS8D-LWE7].

197. *Id.*

highlight the importance of specifying intellectual property rights, establishing (as well as limiting or disclaiming) warranties, restricting activities and uses, and defining the scope and limitations of the user's license to use the software or participate on the platform.[198]

EULA or ToS agreements have become standard and ubiquitous in the age of smartphones.[199] The expectation that Ginormaverse or any virtual world will require such an agreement is hardly surprising. The implications, however, take on additional significance if the metaverse itself becomes ubiquitous and universal. The ToS for a universal platform has the potential to become the equivalent of positive national law. "The vast majority of Americans—97%—now own a cellphone of some kind."[200]

If use of the platform is required by the nation's leading vendors such as Google and Apple, social media giant Facebook, and Microsoft—which remains relevant, if not dominant, in almost every digital sector—along with large retailers including Amazon, Target, and Walmart, it will cover nearly 100% of Americans. The single ToS could end up being required for anyone using a computer operating system (except for those few Linux holdouts that do not also use either Microsoft or Apple), anyone who owns a smart phone, anyone who shops online or uses digital coupons in stores, and so on.[201]

The social pressure on the parties drafting the Ginormaverse ToS may keep the company from overreaching too extensively. At least theoretically, the social backlash from excessive terms and the goal of maintaining customer goodwill has discouraged some of the potentially harmful provisions from becoming standardized in ToS contracts. Back in 2005, the Electric Frontier

198. Abanti Bose, *Advantages and Disadvantages of End-User License Agreements*, IPLEADERS (July 25, 2021), https://blog.ipleaders.in/advantages-disadvantages-end-user-license-agreements/ [https://perma.cc/5EQC-XLYJ]; Jacqueline Gibson, *Q&A What is an EULA?*, LEGALVISION, https://legalvision.com.au/q-and-a/what-is-an-eula/ [https://perma.cc/PD95-Z5UA] ("If you are using an EULA as an addition to an overarching licen[s]e between you and a business, then the EULA will ensure you have recourse to address any issues directly with the individual employees who use the software, rather than only having a legal relationship with the business."); Mike Young, *EULA: 7 Key Parts Of A Software End User License Agreement*, MIKE YOUNG L. FIRM (Nov. 18, 2015), https://mikeyounglaw.com/software-end-user-license-agreement-eula [https://perma.cc/8M7T-CGAA].

199. *Cf.* Annalee Newitz, *Dangerous Terms: A User's Guide to EULAs*, ELEC. FRONTIER FOUND. (Feb. 17, 2005), https://www.eff.org/wp/dangerous-terms-users-guide-eulas [https://perma.cc/Y2WK-4UBL] (perhaps policy makers should have heeded this warning from 2005).

200. *Mobile Fact Sheet*, PEW RSCH. CTR. (June 27, 2021), https://www.pewresearch.org/internet/fact-sheet/mobile/ [https://perma.cc/W96C-X8XX] ("The share of Americans that own a smartphone is now 85%, up from just 35% in Pew Research Center's first survey of smartphone ownership conducted in 2011.").

201. *See* Auxier & Anderson, *supra* note 56.

Foundation warned about EULAs by identifying hidden provisions aimed at stifling consumer criticism, increasing customer monitoring, prohibiting reverse engineering, and modifying both the licensed software and the EULA itself.[202] Although provisions prohibiting reverse engineering and allowing for the modification of software and terms are common, contractual restrictions on consumer feedback have been prohibited by Congress.[203] Nonetheless, the concern remains that provisions in the ToS to compel arbitration and to prohibit class action lawsuits will remove the vast majority of conflicts out of the court system.[204] Whatever efficiency benefits this might provide, it also curtails the development of the common law. If these provisions govern business-to-business transactions as well as business-to-consumer transactions that occur within the virtual world, commercial law could essentially leave the jurisdiction of the courts.

As discussed below, the ToS will be central to identify the scope and ownership of each virtual world user's intellectual property rights, privacy interests, and potential for criminal liability under the Computer Fraud and Abuse Act (CFAA).[205] The ToS will not be able to contractually waive positive law requirements such as those data breach notification statutes or financial regulations, but in many other areas, the ToS can be drafted to supplement or eventually to undermine state and federal law governing the interactions among the members of the public who agree to its terms of service. In addition, as discussed below, the metaphor of a virtual activity may give rise to a very different digital crime than the in-world understanding. For example, digital items can be copied and perhaps criminally or tortiously erased. But despite the virtual world metaphor, an in-world item cannot be stolen because it was never

---

202. Newitz, *supra* note 199.

203. Consumer Review Fairness Act of 2016, 15 U.S.C. §§ 41, 45, 57a (2016) (making void a contract that prohibits consumer reviews, with exceptions for certain types of confidential information); *see* Bill Moak, *Online Reviews: Companies can't bar Consumers from Posting Negative Comments*, CLARION LEDGER (May 24, 2019), https://www.clarionledger.com/story/news/2019/05/24/online-negative-reviews-what-businesses-can-and-cant-do-law-crfa-ftc/3770680002/ [https://perma.cc/AS3L-DA9T].

204. *See, e.g.*, Kater v. Churchill Downs Inc., No. 15-CV-00612-RSL, 2021 WL 511203, at *2 (W.D. Wash. Feb. 11, 2021) (an initial complaint about losing $1,000 in funds on a casino video game ultimately resulted in a class action lawsuit resulting in a $155 million fund, $38,750 in attorneys' fees, and more than 50,000 class members); Kater v. Churchill Downs, No. 3:15-cv-006120RBL, 2018 WL 5734656, at *3 (W.D.Wash. Nov. 02, 2018) (defendant could not both pursue litigation and enforce arbitration provision).

205. *See* 18 U.S.C. § 1030; *see also* Thomas E. Kadri, *Digital Gatekeepers*, 99 TEX. L. REV. 951, 1003 (2021); Orin S. Kerr, *Criminal Law in Virtual Worlds*, 2008 U. CHI. LEGAL F. 423–24 (2008); Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1597 (2003).

a physical object, and the change in access from one user to another may result in a violation of the CFAA or other laws rather than theft.[206]

The ToS will be central to the protection, potential expansion, and rebalancing of intellectual property rights. In this example, Ginormaverse will be the copyright owner of the software and visual images created to own and operate the platform.[207] To permit the interoperability to work, the companies sharing the common platform will need to cross-license the copyrights in their respective audiovisual works as well as in the software code which runs those works.[208] The other vendors will require that the ToS provides that each vendor retains its own copyright, granting a limited, non-exclusive license to Ginormaverse in order to facilitate the interoperability and to standardize the end-user's interactions as each person moves from node to node within the multiverse.

Ginormaverse and the other vendors could choose to make the core code available even more publicly using a Creative Commons license, but history suggests that the code will be protected vigorously from non-partner vendors who do not cross-license their own code.[209] If licensed in this manner, the metaverse will begin to control and exclude which other vendors gain access to the platform. In this way, the interoperable software will work much like the controls used by Google and Apple over their respective app stores.[210]

If history remains any guide, the network effects strongly suggest that while there may be a time of significant experimentation, the benefits of interoperability and access to particularly popular resources along with frictional barriers such as the learning curve for different platforms will result in a very limited number of competitors. There may be a single multiverse, or

206. *See* Kerr, *Criminal Law in Virtual Worlds*, *supra* note 205, at 419, 422–23 (distinguishing violations of rules of play within the virtual world from misuse of credentials to steal funds from attached accounts).

207. *See* 17 U.S.C. § 102 (literary works and audiovisual works); GREG LASTOWKA, VIRTUAL JUSTICE: THE NEW LAWS OF ONLINE WORLDS 170 (2010).

208. Some of the software will not be entirely functional and outside the scope of copyright. Much of the code will be copyright protected, however, requiring cross-licenses.

209. PETE PERLEGOS, CROSS-LICENSING 17 (2005), http://perlegos.com/lawschool/crosslicensing.pdf#page=17 [https://perma.cc/YR5V-G38P] (quoting RICHARD E. CAVES, HAROLD CROOKELL & PETER J. KILLING, THE IMPERFECT MARKET FOR TECHNOLOGY LICENSES, OXFORD BULLETIN OF ECONOMICS AND STATISTICS (1983)).

210. *See, e.g.*, Nikolas Guggenberger, *Essential Platforms*, 24 STAN. TECH. L. REV. 237, 263 (2021) ("Third-party app developers lack practical and reasonable alternatives to the two leading platforms. . . . Moreover, developers remain tied to the app stores beyond the initial download. . . . Google and Apple also compete in the secondary market for apps themselves. Google's apps reach 186 million users, Apple's 105 million.").

like computer operating systems[211] and smartphones,[212] there may be a duopoly, or it may broaden further. In gaming, for example, there are two dominant app stores, but also Steam and the Epic Games Store,[213] and the three major console makers.[214] Netflix and Amazon are also seeking to be competitive in games.[215]

Whether there is one metaverse, a few competing metaverses, or a Web3-inspired multitude of providers, the virtual world will use its ToS to standardize many of the users' expectations within the platform.[216] Areas within the virtual world may have additional restrictions such as specially walled gardens for content screened from young children and areas for only adolescents. Other areas will be screened for the customers of a particular vendor. But these rules will continue to operate within the constraints of the ToS that governs the broader metaverse.

From a contractual standard, this allows the owner of the metaverse to control the virtual space in much the same manner that a mall owner controls the retail space at a mall or the owner of a platform often prioritizes its own

---

211. *See* United States v. Microsoft Corp., 253 F.3d 34, 52 (D.C. Cir. 2001) ("[C]onsumers would not switch from Windows to Mac OS in response to a substantial price increase because of the costs . . . as well as because of the effort involved in learning the new system and transferring files to its format.").

212. *See* Guggenberger, *supra* note 210, at 262 ("Aside from third-party Android stores in China, Google and Apple all but divide up the market for smart phone application platforms with the Google Play Store and the Apple App Store. In 2019, users downloaded 85 billion apps from the Google play store, and 31 billion from the Apple App Store.").

213. *See generally* Andrew Beattie, *How the Video Game Industry Is Changing*, INVESTOPEDIA (Oct. 31, 2021), https://www.investopedia.com/articles/investing/053115/how-video-game-industry-changing.asp [https://perma.cc/JF69-M6P3] ("Tech giants such as Google, Meta [formally Facebook], and Apple, have all made plans to enter the video game industry. . . . Microsoft (MSFT[has already been in the gaming industry through its popular Xbox console."); GRAND VIEW RSCH., GAMING MARKET SIZE, SHARE & TRENDS ANALYSIS REPORT BY DEVICE (CONSOLE, MOBILE, COMPUTER), BY TYPE (ONLINE, OFFLINE), BY REGION (NORTH AMERICA, EUROPE, APAC, LATAM, MEA), AND SEGMENT FORECASTS, 2022 – 2030, https://www.grandviewresearch.com/industry-analysis/gaming-industry?utm_source=prnewswire&utm_medium=referral&utm_campaign=ICT_08-Aug-22&utm_term=gaming_industry&utm_content=rd1 [https://perma.cc/G2YJ-9RXC] ("The global gaming market size was worth 202.64 billion in 2021 and is expected to expand at a compound annual growth rate (CAGR) of 10.2% from 2022 to 2030" or 504.29 billion USD by 2030.).

214. *US Video Gaming Industry in 2022: Gaming Devices & Video Game Content Viewership Trends*, INSIDER INTELLIGENCE (July 21, 2021), https://www.insiderintelligence.com/insights/us-gaming-industry-ecosystem/ [https://perma.cc/7E24-8VSL] ("Gamers turned to their Nintendo, Playstation, and Xbox devices as time spent at home increased in 2020—monthly digital console gamers saw a larger increase than any other gaming device, growing by 6.3% from 2019.").

215. *See* Mike Snider, *Video Games Playing on the Minds of Amazon, Netflix, Peloton and Zoom*, USA TODAY (July 24, 2021), https://www.usatoday.com/story/tech/2021/07/24/amazon-netflix-peloton-zoom-video-games/8070256002/.

216. *See*, *e.g.*, DECENTRALAND, *supra* note 85.

products and services above those of the third-party vendors for which it conducts business.[217] This creates a competitive risk to those companies who rely on the metaverse as a platform from which to conduct business and a tremendous opportunity for the owner of the platform to leverage its own products or services into a prominent position within the virtual world. Ultimately, the success of the metaverse may determine the extent to which antitrust and unfair competition laws are updated to address the practices of the multiverse operators.

For some advocates of NFTs and DAOs, there is an effort to do away with ToS and instead rely on smart contracts. Certainly, no one will miss the need to click through pages of contractual provisions nearly impossible to read as a condition of opening an app or logging into a website. At the same time, however, ToS provide important legal protections for the companies and important warranties for the consumers in e-commerce transactions. DAO owners and the committees or assigned leadership will want contractual waiver to reduce legal risk associated with the metaverse operation.[218] Smart contracts, since they are merely pre-programmed software interactions, do not provide the risk management or contingency planning of true contracts. Perhaps the best example can be seen in the crypto project ICON, which lost 14,000,000 ICX tokens, worth $8 million at the time of the loss, because a programmer noted a software error that permitted the user to mint 25,000 tokens for free on each visit.[219] Had ICON employed a ToS, it could have contractually required users to meet investment criteria. It also could have reserved the power to legally recall and reissue tokens in the event of catastrophic breaches (provided it did so in a way that avoids simply forking the blockchain and causing losses to

---

217. Amazon.com Inc has been repeatedly accused of knocking off products it sells on its website and of exploiting its vast trove of internal data to promote its own merchandise at the expense of other sellers. The company has denied the accusations. But thousands of pages of internal Amazon documents examined by Reuters—including emails, strategy papers and business plans—show the company ran a systematic campaign of creating knockoffs and manipulating search results to boost its own product lines in India, one of the company's largest growth markets.

Aditya Kalra & Steve Stecklow, *The Imitation Game*, REUTERS (Oct. 13, 2021), https://www.reuters.com/investigates/special-report/amazon-india-rigging/ [https://perma.cc/2TJT-LAHU]. *See also* Epic Games, Inc. v. Apple Inc., 493 F. Supp. 3d 817, 828 (N.D. Cal. 2020) ("Epic Games Store was created to compete against the leading multi-publisher digital video game marketplace on computer platforms, Steam, which is operated by Valve Corporation. The Epic Games Store provides access to more than 250 games from more than 200 developers.").

218. *See, e.g.*, DECENTRALAND, *supra* note 85.

219. *Crypto 'Hacker' who Exploited Bug to Mint $17M Could Still Keep It*, PROTOS (Aug. 11, 2021), https://protos.com/crypto-hacker-icon-icx-minted-bug-blockchain-property-right/ [https://perma.cc/K4AK-SVL9]; Birch, *supra* note 72.

other owners' assets).[220] Smart contracting code cannot grant a DAO the legal right to fix software errors, but since software errors are inevitable, metaverse operators will inevitably recognize that legal contracts are more powerful than smart contracts.

In addition, if contractual rights to correct catastrophic software issues are not enough, there are also the myriad of regulatory compliance obligations that the owner of a service must include to ensure that the customers of the service are in compliance with the law and the contractual obligations of the metaverse. Community standards, anti-obscenity and child pornography provisions, copyright notice and takedown disclosures, limitations on investments to accredited or otherwise qualified investors, and many other affirmative obligations must be included in the contracts. As a result, metaverse transactions will likely continue to be governed by contract law in each jurisdiction.

B. Competition Harms and Consumer Protection

A particular concern of the metaverse that may be better addressed through the competition spawned by DAOs and the multiverse is the tendency of enterprises to promote their own activities over those of competitors. In the abstract, this form of self-promotion is entirely reasonable. Nike, for example, will be expected to stock only Nike shoes at its retail stores.[221] There is no consumer or regulatory expectation that it will provide Adidas or Converse sneakers.[222] McDonalds is not obligated to sell Burger King hamburgers, and it can choose to contract with either Pepsi or Coca-Cola for its soft drinks. The right to monopolize one's own stores with one's own goods or services does not seem problematic, and any regulatory intervention would seem absurd.

---

220. *See* Birch, *supra* note 72 ("Poly Network had reported that a person or persons unknown used yet more bugs in smart contracts to redistribute some $600m worth of Ether, Binance Coin and USDC to cryptographically more deserving wallets . . . . Poly Network responded by abandoning code is law and threatening both legal action and direct action . . . .").

221. *See* Stephanie Stoughton & Leslie Walker, *Manufacturers' Online Stores Upset Their Retailers*, WASH. POST (Feb. 8, 1999), https://www.washingtonpost.com/archive/politics/1999/02/08/manufacturers-online-stores-upset-their-retailers/9407a520-6097-4923-9364-1be9aa91ad86/ [https://perma.cc/H3DU-J8Q5] ("Sporting goods retailers were hardly pleased the day Nike Inc. opened its own factory outlets, offering the swoosh-branded athletic shoes at discount prices. . . . Nike's bid to bypass retailers online underscores how the Internet is complicating long-standing business relationships. It is sending tremors through the retailing and manufacturing industries . . . .").

222. *See Refusal to Deal*, FTC, https://www.ftc.gov/tips-advice/competition-guidance/guide-antitrust-laws/single-firm-conduct/refusal-deal [https://perma.cc/89YN-SGF8] ("In general, a firm has no duty to deal with its competitors.").

But the relationship changes when the store both sells goods and competes with the vendors that sell on its platform. Again, it is not a problem new to the internet. Discount stores and department stores have long sold store brands that compete directly with the retailers who market through those chains.[223] It is common practice in the retail industry and has been the subject of FTC scrutiny.

The FTC has outlined situations where the leadership by a retailer's supplier—known as a category captain—might create antitrust concerns. "[T]he category captain might: (1) learn confidential information about rivals' plans; (2) hinder the expansion of rivals; (3) promote collusion among retailers; or (4) facilitate collusion among manufacturers."[224] The first concern regarding confidential information has increased in scope as the economy has shifted to data-driven wholesale and retail strategies.[225] The FTC has been concerned about the ability of category captains to capitalize on their superior market power to dominate the retail space, set preferential pricing arrangement, and artificially heighten barriers to entry for competitors.[226]

The problem becomes significantly worse when the retailer is selling competitors' goods and services, competing with the competitors' goods and services with its own goods, and also serving as the research and promotional platform for those goods and services. In essence, the platform serves as the category captain and the chief rival to the competitors, competitors that are deeply reliant on the platform to provide the marketing and distribution. For example, in terms of smartphone, tablet, and computer apps, Google Play hosts approximately 3.5 million apps, Apple App Store houses 2.23 million apps, Windows Store hosts 669,000, and Amazon Appstore has 476,000.[227]

---

223. *See* Gregory Gundlach & Alex Loff, *Competitive Exclusion In Category Captain Arrangements* 7 (Aug. 18, 2018) (Antitrust Inst., Working Monograph), https://www.antitrustinstitute.org/wp-content/uploads/2018/10/Gundlach-and-Loff_Comp-Exc.-in-Cat-Cap_8.31.18-FINAL.pdf [https://perma.cc/EL2D-GSAQ] ("The most popular approach to category management involves 'outsourcing' decisions to a single manufacturer in the category (a.k.a., the 'category captain'). . . . The extent of involvement and the level of influence and control held by a category captain can be extensive."); *see also* Bradley J. Lorden, *Category Management: The Antitrust Implications in the United States and Europe*, 23 LOY. CONSUMER L. REV. 541, 541–42 (2011).

224. Lorden, *supra* note 223, at 545 (quoting FED. TRADE COMM'N, REPORT ON THE FEDERAL TRADE COMMISSION WORKSHOP ON SLOTTING ALLOWANCES AND OTHER MARKETING PRACTICES IN THE GROCERY INDUSTRY 50 (2001)).

225. *See* Guggenberger, *supra* note 210, at 265, 266.

226. *See generally* Stéphane Caprice & Vanessa von Schlippenbach, *Consumer Shopping Costs as a Cause of Slotting Fees: A Rent-Shifting Mechanism* (Deutsches Institut für Wirtschaftsforschung, Working Paper No. 1020, 2010), https://econpapers.repec.org/RePEc:diw:diwwpp:dp1012 [https://perma.cc/B9RQ-3R9U].

227. *Number of Apps Available in Leading App Stores as of Q2 2022*, STATISTICA (Aug. 11, 2022), https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/ [https://perma.cc/6PCS-4TN5].

With millions of apps being hosted, the search algorithms and recommendations are essential for companies to connect with customers. "But as Apple has become one of the largest competitors on a platform that it controls, suspicions that the company has been tipping the scales in its own favor are at the heart of antitrust complaints . . . ."[228] If competitors wish to improve their placement, they have the option of paying Apple for that priority.[229]

Apple is not alone in prioritizing its own products, charging its competitors, and potentially using customer data for competitive advantage. Amazon, the nation's leading retailer, has claimed this title as well.[230] "[I]nternal documents also show that Amazon employees studied proprietary data about other brands on Amazon.in, including detailed information about customer returns. The aim: to identify and target goods—described as 'reference' or 'benchmark' products—and 'replicate' them."[231] For wholesalers and retailers, the transactions with Amazon are a devil's bargain. "53% of vendors see themselves in direct competition with Amazon's products."[232]

Meta has been the subject of similar accusations. In August 2021, the FTC updated its complaint against Meta (then Facebook) over its innovation strategies.[233] When Facebook was unable to develop its own apps to compete in the mobile marketplace, "Facebook instead resorted to an illegal buy-or-bury scheme to maintain its dominance. . . . And to further moat its monopoly,

228. Jack Nicas & Keith Collins, *How Apple's Apps Topped Rivals in the App Store It Controls*, N.Y. TIMES (Sept. 19, 2019), https://www.nytimes.com/interactive/2019/09/09/technology/apple-app-store-competition.html [https://perma.cc/89KT-AVXY].

229. *Id. See* Guggenberger, *supra* note 210, at 266.

230. See Aditya Kalra & Steve Stecklow, supra note 217; Karen Weise, Prime Power: How Amazon Squeezes the Businesses Behind Its Store, N. Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/2019/12/19/technology/amazon-sellers.html [https://perma.cc/B9DK-V6MN] ("Last year, Americans bought more books, T-shirts and other products on Amazon than eBay, Walmart and its next seven largest online competitors combined, according to eMarketer, a research company.").

231. Kalra & Stecklow, *supra* note 217, at 3.

232. Guggenberger, *supra* note 210, at 259 (citing JUNGLE SCOUT, THE STATE OF THE AMAZON SELLER 2020 24 (2020), https://www.junglescout.com/wp-content/uploads/2020/02/State-of-the-Seller-Survey.pdf [https://perma.cc/SL55-XDU4]).

233. *See* Plaintiff's First Amended Complaint for Injunctive and Other Equitable Relief at 1, FTC v. Facebook, Inc., No. 1:20-cv-03590-JEB (D.D.C. Aug. 19, 2021) [hereinafter FTC Amended Complaint] ("Facebook has maintained its monopoly position in significant part by pursuing Chief Executive Officer ("CEO") Mark Zuckerberg's strategy, expressed in 2008: 'it is better to buy than compete.' ").

Facebook lured app developers to the platform, surveilled them for signs of success, and then buried them when they became competitive threats."[234]

Nor should Google be left off the list of self-dealing platforms, at least according to allegations at the heart of recent litigation involving Epic Games over the placement of *Fortnite* in the Google Play Store. According to the complaint, Google had been willing to arrange a side-deal with Epic over the percentage of fees charged, had arranged for payments to rival game company Blizzard, increased restrictions on side-loading apps to stop circumvention of the Play Store monopoly, and undertaken additional anticompetitive strategies.[235]

These efforts, and many like them, have been the result of the anticompetitive behavior of platforms because, much like scorpions, it is simply in their nature. "[P]latform providers work to define both collected data and algorithmic logics as zones of exclusivity. In particular, platforms use contracts systematically to facilitate and protect their own legibility function, extracting transparency from users but shielding basic operational knowledge from third-party vendors, users, and advertisers alike."[236]

The future is already here.

> Over the last two decades, digital platforms have become crucial marketplaces that bring together demand and supply of goods and services online. . . . They have gained systemic relevance and shape the global economy. . . . As of August 2020, they represent an aggregate market valuation of $8.2 trillion.[237]

---

234. Press Release, FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate, FTC (Aug. 19, 2021), https://www.ftc.gov/news-events/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush [https://perma.cc/QAE4-EJN9].

235. Plaintiff's First Amended Complaint for Injunctive Relief, 32, Epic Games, Inc. v. Google, LLC, No. 3:20-CV-05671-JD (No. 165-10) (N.D. Cal. Aug. 20, 2021) [hereinafter Epic Amended Complaint]; *see* Sean Hollister, *The* Epic v. Google *Lawsuit Finally Makes Sense*, THE VERGE (Aug. 19, 2021), https://www.theverge.com/2021/8/19/22632804/epic-google-lawsuit-unredacted-complaint-antitrust [https://perma.cc/5BAY-EVDD].

236. Julie E. Cohen, *Law for the Platform Economy*, 51 U. C. DAVIS L. REV. 133, 154 (2017).

> [Epic] alleges the company was so worried about Epic setting a precedent by abandoning the Play Store that it [Google] unleashed a broad effort to keep developers from following the company's lead. That included straight-up paying top game developers, including Activision Blizzard to stick around, and sharing additional chunks of its revenue with phone makers if they agreed not to preinstall any other app stores.

Hollister, *supra* note 235.

237. Guggenberger, *supra* note 210, at 253–54.

For platforms, the markets are driven by scale and fueled by network effects.[238] "Strong network effects can insulate a dominant personal social networking provider from competitive threats until a disruptive or innovative technology emerges to open up new ways for users to connect."[239] Of course, while network effects are necessary to build a use case for a network, network effects are not themselves sufficient, which is why companies resort to anticompetitive practices to add additional competitive barriers, discourage participants from leaving the networks, and forestall effective competition from emerging.[240]

These digital platforms are striving to control Ginormaverse, and they are likely to use competitive barriers, customer retention strategies, and buyouts to maintain their advantage. Unsurprisingly, Web3 advocates are hoping to keep this power out of their hands. The future of the metaverse will not turn on any one competitive advantage, however, for as the Epic Games litigation highlights, Android's open-sourced operating system and the open architecture of Android smartphones has been as successful as Apple and Amazon at controlling the operating environment, exploiting the transactional data, and crafting barriers to competition that empower the operational leadership to dominate.[241]

As a result, any planning for the metaverse must take the potential consumer harms for anticompetitive behavior into account, *ex ante*, before the model has become too big to fail. Whether the enforcement is developed through smart contracts, terms of service, or updated antitrust guidance, the bright-line prohibition should be clear that a company which provides another company's

---

238. *See* D'Arcy Coolican & Li Jin, *The Dynamics of Network Effects*, ANDREESSEN HOROWITZ (Dec. 13, 2018), https://a16z.com/2018/12/13/network-effects-dynamics-in-practice/ [https://perma.cc/LNX9-2QLJ] ("The most successful companies and products of the internet era have all been predicated on the concept of network effects, where the network becomes more valuable to users as more people use it.").

239. FTC Amended Complaint at 3, *supra* note 233. *But see* Coolican & Jin, *supra* note 238 (going beyond the assumption that each member of a network contributes equally to that network, increasing the network's value and competitive advantage to explore differences and limitations within the network).

240. *See* Catherine Tucker, *Network Effects and Market Power: What Have We Learned in the Last Decade*, TECH. & RSCH. POL'Y INITIATIVE, Spring 2018, at 72, 73–74 (2018) https://sites.bu.edu/tpri/files/2018/07/tucker-network-effects-antitrust2018.pdf [https://perma.cc/UCM2-D9HA] (discussing how the absence of "sunk costs" enables network users to move rapidly from network to network). Earlier models of network effects presumed hardware costs, user interface learning curves, and time establishing accounts as investments or sunk costs that would likely retain customers. *Id.* In social media competition, these are largely absent. *Id.*; Coolican & Jin *supra* note 238.

241. Epic Amended Complaint, *supra* note 235, at 8.

goods or services should be precluded from competing with that company. Any company can provide the platform and any company can compete on the platform, but it is intrinsically anticompetitive to do both, and over time, the network benefits of such competitive advantage will squeeze most competition out of the marketplace.

The limitation on self-preference is essential for the metaverse to meet its potential. In many ways, the metaphor of the virtual world is little more than a visualized search function. Information, entertainment, contacts, products, and services are all found for the user based on the search criteria and prior behavior of that user. Ginormaverse will be the gateway to the information a person needs each day. In that way, it will be much like Google is today. As of 2020, for example, "across all platforms, including mobile and tablet, the Google's share hovers . . . at 88%."[242] It helped that Google bought the exclusive right to be the default search engine on Apple operating systems and tied its search engine to its own operating system, Android. Whether Google maintains that dominance into the metaverse or a competitor replaces it, the potential to prioritize and define the user experience will be tremendous. Only through contractual and legal restrictions can this power be diffused.

C. Copyright

Because Ginormaverse is an interoperable platform, the ToS would likely allow users to own the intellectual property rights in their avatar.[243] Like most games and virtual worlds, there would be free and low-cost stock avatars available as well, but the users will likely wish to customize one or more avatars, meaning that they would want the ability to use these in any interoperable space.[244] The right to retain copyright and other intellectual property rights will be even more important to other assets beyond the avatars.

Although Ginormaverse will likely allow users to keep the copyright in their works, the users will also need to warrant that they have the rights to the

---

242. Guggenberger, *supra* note 210, at 269 (citing *Search Engine Market Share United States of America,* STATCOUNTER GLOB. STATS, https://gs.statcounter.com/search-engine-market-share/all/united-states-of-america [https://perma.cc/YFQ6-TCBE]).

243. *See* Kevin Dong, *Developing A Digital Property Law Regime*, 105 CORNELL L. REV. 1745, 1750–51 (2020) ("[V]irtual items are instead governed by the laws of intellectual property and contracts."); Kenneth W. Eng, *Content Creators, Virtual Goods: Who Owns Virtual Property?*, 34 CARDOZO ARTS & ENT. L.J. 249, 252 (2016) ("[T]he law should first identify virtual goods that warrant ownership rights and then extend copyright law to grant ownership protection to the end-user.").

244. *See* Heather Mueller, *What is Software Interoperability and How Can It Boost Profits and Productivity?*, FORMSTACK (June 24, 2021), https://www.formstack.com/resources/blog-software-interoperability [https://perma.cc/5ATM-QGCW].

copyrighted materials used in the avatars and other content utilized within the virtual world. The ToS will likely include specific representations and warranties indemnifying Ginormaverse from any infringements by the users. To the extent that Ginormaverse represents multiple copies of the content needed to provision each user interaction on primary and secondary computer servers, back-up systems, and cached systems used to reduce loading times, a particular copyrighted work might be replicated numerous times within Ginormaverse's computer system. The ToS should take these reproductions, archival copies, and public performances into account in the license from each consumer and business activity utilizing the system.

For example, the Virtual Reality Church has been in operation since 2016.[245] According to its pastor, D.J. Soto, "the spiritual connection people experience in person in church, is equally accessible in virtual reality. 'We believe God is everywhere, he's in physical dimensions, spiritual dimensions, and virtual reality.' "[246] Unlike a Zoom-based congregation, the participants wearing VR goggles will be unable to read a print copy of their prayer book to use during the service. To accommodate the need for prayer books within the VR experience, the church should have a license from the publisher to provide those works to parishioners within the VR environment. In a similar manner, the sermons and homilies written by clergy for their online congregations will be protected by copyright as soon as they are created, and the ToS should not transfer that copyright from the author to the owners of Ginormaverse or other platforms.

This will be equally true for all corporate documents, presentations, educational materials, and other types of content created by individuals or enterprises for presentation, discussion, or distribution within the virtual world. Some of these works will also embody trade secrets, and potentially some of these works could include attorney-client privileged content or attorney work

245. Chace Beech, *Virtual Reality Church Brings Worship to New Dimensions*, SPECTRUM NEWS 1 (Mar. 15, 2021), https://spectrumnews1.com/ca/la-west/technology/2021/03/14/virtual-reality-church-brings-worship-to-new-dimensions [https://perma.cc/4X7K-NQ9A] ("VR Church is designed, built, and run entirely online. It was founded in 2016 by D.J. Soto, an ordained Bishop. He was experimenting with virtual reality and realized he could marry this new technology with his religious work.").

246. *Id.* (quoting Bishop Soto).

product.[247] Virtual doctor visits might use cameras rather than avatars, but could still include medical records subject to HIPAA privacy and security rules.[248]

D. Confidentiality and Privacy

The importance of confidentiality and data security are more explicit when the documents are governed by federal privacy laws such as the HIPAA privacy rule[249] or the Gramm-Leach-Bliley financial privacy rules,[250] but these concerns are nearly as significant for any business operating within Ginormaverse that is concerned about its trade secrets and confidential data.[251]

---

247. On August 10, 2008, the Section presented a panel program entitled "Real Concerns When Practicing in Virtual Worlds" at the ABA Annual meeting in New York City. . . . Benjamin Duranske talked about some of the ethical concerns of lawyer participation in virtual worlds. Because a virtual worlds provider may have the ability to review logs of attorney conversations, and other avatars may have the ability to intercept communications, attorney-client communications in virtual worlds may not have the protection of the attorney-client privilege. Also, issues of unauthorized practice of law arise with the question of "where are you practicing" when a lawyer in one jurisdiction speaks in a virtual world with a client from another jurisdiction. Given these issues, he advises lawyers not to give advice in today's virtual worlds. He cautioned that if a lawyer would not say something in an email, he or she should not say the same thing in a virtual world.

Stephen S. Wu, *Real Concerns When Practicing in Virtual Worlds*, ABA SCITECH LAW, Winter 2009 at 19, 24–25.

248. *See* Stephanie Murtagh & Jasmine M. Fisher, *Compliance Considerations: Access to Telehealth Services for Patients with Disabilities*, J. HEALTH CARE COMPLIANCE, July–Aug. 2021 at 5, 6–7 (2021) (discussing HIPAA waivers for telemedicine during the COVID-19 pandemic); *see also* Joshua A.T. Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, 2 U.C. IRVINE L. REV. 695, 735 (2012) ("If a game god were to alter its EULA or TOS to include the kind of general standardized consent to human subjects research that the ANPRM contemplates, the user would not have a meaningful opportunity to decline. The user would have to either agree to the changed EULA or give up all of his or her online community, property, and account progress."); Rebecca Crootof & BJ Ard, *Structuring Techlaw*, 34 HARV. J.L. & TECH. 347, 357 (2021) (exploring range of legal protections).

249. Health Insurance Portability and Accountability Act (HIPAA), 45 C.F.R. §§ 160.103, 164.514 (2018). *See generally*, Charlotte A. Tschider, *Regulating the Internet of Things: Discrimination, Privacy, and Cybersecurity in the Artificial Intelligence Age*, 96 DENV. L. REV. 87, 95 (2018) ("Large data volumes also enable data aggregation for purposes of sale, transfer, and exchange."). Although this Article was looking at the data implications outside of virtual worlds, many of the concerns are fully applicable to these systems.

250. Gramm-Leach-Bliley Act (GLBA), 15 U.S.C. § 6802.

251. Certain corporate assets, such as databases of customer information and preferences, are valuable only because of their confidentiality. One data breach could greatly diminish the value of such an intangible asset. For example, the damage that a corporate insider can generate in one episode of information theft has been, in at least one instance, approximated to be between $50 million to $100 million. Similarly,

Federal law provides that trade secret "means all forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible . . . ."[252] A trade secret requires two additional criteria to be protected. First, "the owner thereof has taken reasonable measures to keep such information secret;" and second, "the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from the disclosure or use of the information."[253] "Commentators universally agree that the [Uniform Trade Secret Act's] independent economic value requirement was intended to codify the common law's requirement that a trade secret give its owner a 'competitive advantage' over others who do not know or use it."[254]

The basic requirements of trade secret protection, therefore, require that the virtual platform and the users of the virtual platform agree to respect the trade secrets of their respective owners.[255] Incorporating the duty to protect trade secrets into the ToS will solve one aspect of trade secret practice focused on the explicit duty of all parties subject to the agreement to respect *bona fide* trade secrets. At the same time, however, it does raise some additional concerns.

Trade secrets, confidential information, HIPAA protected health care records, and similar data all have the need for both legal protection from

---

> corporate proprietary information protected solely by trade secret law could, in effect, lose all its value in an information crime incident . . . .

See Andrea M. Matwyshyn, *Material Vulnerabilities: Data Privacy, Corporate Information Security, and Securities Regulation*, 3 BERKELEY BUS. L.J. 129, 139–40 (2005).

252. 18 U.S.C. § 1839(3) (defining trade secret); s*ee* Eric R. Claeys, *The Use Requirement at Common Law and Under the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 583, 583–84 (2010); *see also* Unif. Trade Secrets Act § 1(4) (Unif. L. Comm'n 1985) (same).

253. 18 U.S.C. § 1839(3)(A)–(B).

254. Camilla A. Hrdy & Mark A. Lemley, *Abandoning Trade Secrets*, 73 STAN. L. REV. 1, 26 (2021).

255. *See* Sharon K. Sandeen, *The Evolution of Trade Secret Law and Why Courts Commit Error When They Do Not Follow the Uniform Trade Secrets Act*, 33 HAMLINE L. REV. 493, 499 (2010).

> The existence of secret information coupled with an express or implied agreement of confidentiality made it easy for common law courts to impose liability on individuals or companies who were parties to the agreement because breach of contract and breach of trust were well-recognized wrongs. The more difficult issue for some courts was to determine if secret information actually existed. This led to the development of principles for differentiating between protectable information and unprotectable information, including the concept of reasonable efforts to maintain secrecy.

Id.

unauthorized access and a pragmatic prohibition against unauthorized use. While these concerns overlap, they are not necessarily the same. HIPAA rules, for example, allow third parties to access protected records for payment, treatment, and health care operations.[256] Attorneys share client records with paralegals, staff, printers, and others to the extent necessary to provide the needed legal services.[257] Ginormaverse, as the platform, will have access to any and all information that parties share across the system. To minimize the usability of the data by the platform, its employees, and any third parties supporting the hardware and technology, encryption tools will be required to restrict access and readability of the data while stored and to limit the readability of the data to only the parties when it is being used. To the extent technologically feasible, only the authorized users should be able to access, decipher, read, or transfer confidential documents within Ginormaverse. Confidential discussions and videos should not be retained after the session unless specifically requested.[258] And when any audio or video engagements are recorded, they should only be accessible by the parties themselves. In no case should the content be available to Ginormaverse for training or quality assurance purposes.

The robust privacy and security requirements are one of the many reasons that each user must be individually identified. While true anonymity may be appropriate for select gaming, media, and perhaps adult-entertainment activities, those activities that require credentialed access to content and engagements will need to have a mechanism of verifying the identity for each participant. This is relatively straight-forward to accomplish in a closed system where the information is held in confidence by the vendor. In an interoperable and permeable network, the use of blockchain technologies or other forms of distributed ledger may be part of the solution.

---

256. 45 C.F.R. § 164.506 (2017) (stating the regulations further limit the extent of disclosures to the minimum necessary to carry out the requirements).

257. *See, e.g.*, ABA MODEL RULES OF PRO. CONDUCT r. 1.6 (AM. BAR ASS'N 2020)

> Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

ABA MODEL RULES OF PRO. CONDUCT r. 1.6 cmt. 18 (AM. BAR ASS'N 2020), https://www.americanbar.org/groups/professional_responsibility/publications/model_rules_of_professional_conduct/rule_1_6_confidentiality_of_information/comment_on_rule_1_6/ [https://perma.cc/KN5E-P78V].

258. Digital media are generally fixed upon creation and stored, at least temporarily, while being transmitted in a close approximation of real time.

E. Rights to Biometrics, Names, Images, and Likenesses

To identify a person in the real world, other people use their visual looks, the sound of their voice, and other physical attributes. Ginormaverse will need to acquire a limited license to use the name, image, and likeness of each user of the system. Absent such a license, there is the potential for the virtual world to be violating the legal protections for the customer's biometric data[259] and for their rights of publicity.[260]

Capturing the biometric data regarding a person's visual looks, voice, fingerprints, eye-prints, or other unique identifiers is governed in some states under biometric notification and use laws.[261] By December 2021, there were more than ten states with biometric privacy laws of various types, with provisions that vary considerably.[262] At the end of 2021, nearly two dozen states had additional laws under consideration.[263]

Although the biometric data protection laws vary considerably from state to state, they all require some level of notice to the individual before the person's biometric information is collected and stored.[264] The Illinois Biometric

---

259. Molly DiRago & Troutman Pepper, *The Litigation Landscape of Illinois' Biometric Information Privacy Act*, AM. BAR ASS'N (Aug. 20, 2021), https://www.americanbar.org/groups/tort_trial_insurance_practice/committees/cyber-data-privacy/the-litigation-landscape/ [https://perma.cc/FL4W-YJSE]

> Illinois was the first state to regulate the collection and storage of biometric data. Generally, BIPA requires any private entity in possession of biometric information to: (i) develop a written policy, (ii) inform the owner of the biometric information in writing about the purpose for collecting the information and the length of time it will be stored, (iii) obtain written consent for the collection and storage of the data, and (iv) refrain from selling, leasing, trading, or otherwise profiting from that biometric information.

Id.

260. *See* No Doubt v. Activision Publ'g, Inc., 122 Cal. Rptr. 3d 397, 411 (Cal. Ct. App. 2011) ("[T]hat the avatars appear in the context of a video game that contains many other creative elements, does not transform the avatars into anything other than exact depictions of No Doubt's members doing exactly what they do as celebrities."); *In re* NCAA Student-Athlete Name & Likeness Licensing Litig., 724 F.3d 1268, 1276 (9th Cir. 2013) (quoting *No Doubt*, 122 Cal. Rptr. 3d at 411 for the same proposition).

261. *See* Lauren Caisman, Amy de la Lama, Melissa Ruth Whigham & Bryan Cave Leighton Paisner, *U.S. Biometric Laws & Pending Legislation Tracker*, JD SUPRA (May 13, 2021), https://www.jdsupra.com/legalnews/u-s-biometric-laws-pending-legislation-5729436/ [https://perma.cc/5EVJ-Q6DF] ("Biometric privacy laws and regulations generally require businesses to track, inform employees or consumers of, and provide methods for employees or consumers to consent to, the collection of biometric information or biometric identifiers.").

262. *Id.*

263. *Id.*

264. *See* DiRago & Pepper, *supra* note 259.

Information Privacy Act (BIPA)[265] became the most significant of these laws, in part because liability could arise from violations of the law without the need to show additional damages.[266] The laws generally require some explanation of the use to which the biometric information will be put by the enterprise collecting the information, and the laws may include limitations on the use of the data.[267]

In addition to biometric data, there are also legal restrictions on the commercial use of a person's name, image, and likeness.[268] In a virtual world, these may overlap with the person's biometric data, but in other situations, these rights will be complementary. The right to protect against the unauthorized commercial exploitation of one's name or likeness evolved under different names during the nineteenth century and distilled into the law of privacy as a result of the seminal law review article by Samuel Warren and Louis Brandeis.[269] Although the precise contours of the law have never been uniformly agreed upon by the states, rights of publicity have been recognized by the Supreme Court.[270] Copyright scholar Melville Nimmer[271] and Torts expert Dean William Prosser[272] each further developed the conceptual

---

265. 740 ILL. COMP. STAT. 14/1 (2008).

266. Rosenbach v. Six Flags Ent. Corp., 129 N.E.3d 1197, 1206 (Ill. 2019) ("The duties imposed on private entities by section 15 of the Act (740 ILL. COMP. STAT. ANN. 14/15 (West 2016)) regarding the collection, retention, disclosure, and destruction of a person's or customer's biometric identifiers or biometric information define the contours of that statutory right.").

267. *See* DiRago & Pepper, *supra* note 259.

268. *See e.g.*, CAL. CIV. CODE § 3344 (West 2022); N.Y. CIV. RIGHTS LAW §§ 50–51 (McKinney 2021).

269. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890); *see also* Pavesich v. New England Life Ins. Co., 50 S.E. 68, 80–81 (Ga. 1905) (the first case to recognize the common law right of publicity in the United States); Roberson v. Rochester Folding Box Co., 64 N.E. 442, 447 (N.Y. 1902) (rejecting the intermediate court's recognition of commercial privacy and leading to the legislative adoption of N.Y. CIV. RIGHTS LAW §§ 50-51 (McKinney 1905)).

270. Zacchini v. Scripps-Howard Broad. Co., 433 U.S. 562, 580 (1977) (upholding right of publicity claim over news station claim of First Amendment right to air an entire performance as a human cannonball). Most recently, the Supreme Court obliquely supported rights of publicity, as exploited by student athletes. *See* Nat'l. Collegiate Athletic Ass'n. v. Alston, 141 S. Ct. 2141, 2166 (2021) ("By permitting colleges and universities to offer enhanced education-related benefits, its decision may encourage scholastic achievement and allow student-athletes a measure of compensation more consistent with the value they bring to their schools.").

271. Melville B. Nimmer, *The Right of Publicity*, 19 LAW & CONTEMP. PROBS. 203 (1954).

272. William Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960); *see* Christine DiGregorio, *Finding A Fair Balance for the Right of Publicity and First Amendment Protections*, 33 TOURO L. REV. 995, 1000 (2017).

> Prosser . . . categorized it into four distinct torts: intrusion to solitude, public

framework even as courts were struggling to both recognize the fundamental right and balance it against federal law's expanding free speech jurisprudence and copyright law.

Publicity rights grew in scope along with the power of media, increasingly as a common law development. In *Haelan Laboratories v. Topps Chewing Gum*,[273] the courts clarified the scope of the increasingly important common law right.

> We think that, in addition to and independent of that right of privacy (which in New York derives from statute), a man has a right in the publicity value of his photograph, i.e., the right to grant the exclusive privilege of publishing his picture . . . .
>
> . . . .
>
> This right might be called a "right of publicity." For it is common knowledge that many prominent persons (especially actors and ball-players), far from having their feelings bruised through public exposure of their likeness, would *feel sorely deprived if they no longer received money* for authorizing advertisements, popularizing their countenances, displayed in newspapers, magazines, buses, trains and subways.[274]

As corporations have monetized the rights of their customers and social media has created a massive new marketplace for exploitation of these rights, each member of the public has the potential to gain economic value—or at least to recognize an injustice when someone else exploits their name, image, or likeness—for commercial advantage.[275]

The tension among rights of publicity and the associated biometric data protections, the rights of copyright, and the rights of free speech have been addressed in a variety of balancing tests. These include the Second Circuit's

---

> disclosure of embarrassing private facts, false light in the public eye, and appropriation of one's name and likeness for the defendant's advantage. Prosser defined his fourth category as a "defendant making use of the name to pirate the plaintiff's identity for some advantage of his own;" this later became known as the right of publicity.

Id.

273. 202 F.2d 866 (2d Cir. 1953).

274. *Id*. at 868 (emphasis added).

275. *See* Jennifer E. Rothman, *The Inalienable Right of Publicity*, 101 GEO. L.J. 185, 227 (2012) ("The right of publicity encompasses rights far beyond the mere collection of income and entitlement to the economic value that flows from uses of a person's identity. The right of publicity provides control over the use of a person's identity and, therefore, ultimately over the person herself."); Jon M. Garon, *Commercializing the Digital Canvas: Renewing Rights of Attribution for Artists, Authors, and Performers*, 1 TEX. A&M L. REV. 837, 838–39 (2014). In contrast, other scholars are strong critics of these rights. *See*, *e.g.*, Michael Madow, *Private Ownership of Public Image: Popular Cultural and Publicity Rights*, 81 CALIF. L. REV. 125, 178–79 (1993).

Rogers Test,[276] the California and Ninth Circuit's Transformative Use Test,[277] the Missouri Supreme Court Predominant Use Test,[278] copyright preemption,[279] news reporting exceptions,[280] and similar limitations.[281]

California provides representative formulations of both the common law and statutory rights of publicity.

> The elements of a right-of-publicity claim under California common law are: "(1) the defendant's use of the plaintiff's identity; (2) the appropriation of plaintiff's name or likeness to defendant's advantage, commercially or otherwise; (3) lack of consent; and (4) resulting injury." The same claim under California Civil Code § 3344 requires a plaintiff to prove "all the elements of the common law cause of action" plus "a knowing use by the defendant as well as a direct connection between the alleged use and the commercial purpose."[282]

The Restatement (Second) of Torts provides simply that "[o]ne who appropriates to his own use or benefit the name or likeness of another is subject to liability to the other for invasion of his privacy."[283]

Rather than focusing on the commercial exploitation of one's name or likeness, comment b to the Restatement suggests an even more expansive reading:

> The common form of invasion of privacy under the rule here stated is the appropriation and use of the plaintiff's name or likeness to advertise the defendant's business or product, or for some similar commercial purpose. Apart from statute, however, the rule stated is not limited to commercial appropriation. It applies also when the defendant makes use of

---

276. Rogers v. Grimaldi, 875 F.2d 994, 999 (2d Cir. 1989).

277. Comedy III Prod., Inc. v. Gary Saderup, Inc., 21 P.3d 797 (Cal. 2001).

278. Doe v. TCI Cablevision, 110 S.W.3d 363, 374 (Mo. 2003).

279. *In re* Jackson, 972 F.3d 25, 33 (2d Cir. 2020) (Rapper Curtis James Jackson III's "use of his voice on Roberts' mixtape is preempted by the express terms of § 301 of the Copyright Act. . . . [I]mplied preemption precludes the application of state laws to the extent that those laws interfere with or frustrate the functioning of . . . the Copyright Act.").

280. Time, Inc. v. Hill, 385 U.S. 374, 397 (1967) ("That books, newspapers, and magazines are published and sold for profit does not prevent them from being a form of expression whose liberty is safeguarded by the First Amendment.") (internal quotation marks omitted) (quoting Joseph Burstyn, Inc. v. Wilson, 343 U.S. 495, 501–02 (1952).

281. *See*, *e.g.*, Martin H. Redish & Kelsey B. Shust, *The Right of Publicity and the First Amendment in the Modern Age of Commercial Speech*, 56 WM. & MARY L. REV. 1443 (2015).

282. *In re* NCAA Student-Athlete Name & Likeness Licensing Litig., 724 F.3d 1268, 1273 n.4 (9th Cir. 2013) (internal quotation marks omitted) (quoting Stewart v. Rolling Stone LLC, 105 Cal. Rptr. 3d 98, 111 (2010)).

283. RESTATEMENT (SECOND) OF TORTS § 652C (AM. L. INST. 1977).

> the plaintiff's name or likeness for his own purposes and benefit, even though the use is not a commercial one, and even though the benefit sought to be obtained is not a pecuniary one. Statutes in some states have, however, limited the liability to commercial uses of the name or likeness.[284]

Despite the California language that the rights of publicity can be exploited "commercially or otherwise" and Restatement section 652C's suggestion that only state statutes limit rights of publicity to commercial activity, these are usually (but not always) a strong demarcation. Two cases highlight what has been commonly understood to demark the claims.

The leading case involved the nephew of matinee idol Rudolph Valentino. Since the common law rights of publicity evolved out of privacy rights, they do not generally survive the death of the individual.[285] Nonetheless, a concurrence by a majority of the California Supreme Court tried to make clear that rights of publicity do not extend into communicative works.

> While few courts have addressed the question of the parameters of the right of publicity in the context of expressive activities, their response has been consistent. Whether the publication involved was factual and biographical or fictional, the right of publicity has not been held to outweigh the value of free expression. Any other conclusion would allow reports and commentaries on the thoughts and conduct of public and prominent persons to be subject to censorship under the guise of preventing the dissipation of the publicity value of a person's identity. Moreover, the creation of historical novels and other works inspired by actual events and people would be off limits to the fictional author. An important avenue of self-expression would be blocked and the marketplace of ideas would be diminished.[286]

The California Supreme Court made very clear in 1979 that the First Amendment concerns at the heart of limitations to common law defamation and privacy applied with equal vigor to claims for the rights of publicity. The concurrence also rejected an attempt to interject the inapplicable "actual malice" standard,[287] instead recognizing the need for adaptation and story-telling using fictionalized accounts would make the use of the actual malice

---

284. *Id*. at cmt. b.

285. Guglielmi v. Spelling-Goldberg Prod., 603 P.2d 454, 455 (Cal. 1979); Lugosi v. Universal Pictures, 603 P.2d 425, 431 (1979).

286. *Guglielmi,* 603 P.2d at 461–62 (Bird, C.J., concurring).

287. *See* N.Y. Times Co. v. Sullivan, 376 U.S. 254, 267 (1964) (holding the speech of public figures is subject to actual malice standard).

standard more confounding than helpful.[288] Although the concurrence was largely dicta, it demonstrated a clear distinction between communicative works of fact and fiction for which there were no publicity rights and the commercial products, ads, and endorsements for which there would continue to be protection from commercial appropriation.

The *Guglielmi v. Spelling-Goldberg Prod.* Court also distinguished the rather unique theft involved in *Zacchini v. Scripps-Howard Broad*. The Supreme Court relied on state law protection for "the 'right to the publicity value of his performance,' the right to control its commercial display and exploitation."[289] Unlike a name or likeness misappropriation, the value of a person's performance may well be protected by statute or common law. It may even be an implicit extension of the right of publicity, but it is also an economic right about taking the value of another's work without authorization. At the heart of *Zacchini* is the same economic theft that is central to the core of rights of publicity actions, and which is distinct from free speech uses where a person's true or fictionalized story is incorporated into a story being told by a third party.

These themes have been repeated in later California case law. In *Sarver v. Chartier*,[290] the Ninth Circuit rejected a former army sergeant's claim that he had been falsely portrayed in the movie *The Hurt Locker*.[291] He had not consented or licensed his publicity rights to the producers.[292] Dismissing all his claims under the California anti-SLAPP statute,[293] the court noted "*The Hurt Locker* is not speech proposing a commercial transaction."[294] Following *Guglielmi,* the court rejected all claims. Nearly a decade later, Olivia De Havilland brought a similar set of complaints for a portrayal she considered

---

288. *See* Time, Inc. v. Hill, 385 U.S. 374, 397 (1967) (holding privacy claims, though non-defamatory, remain subject to actual malice standard); Hustler Magazine, Inc. v. Falwell, 485 U.S. 46, 56 (1988) (holding actual malice standard is used for intentional parody).

289. *Guglielmi*, 603 P.2d at 464 (quoting Zacchini v. Scripps-Howard Broad, 433 U.S. 562, 565 (1977)). In *Zacchini*, the live performance of the Human Cannon Ball was filmed and aired in its entirety on a segment of the local news, having the potential to reduce greatly the public's interested in attending the event as live spectators. *See generally Zacchini*, 433 U.S. 562 (1977). This was a commercial harm, according to the Supreme Court, notwithstanding that it was committed in the form of a media broadcast. *Id.* at 580.

290. 813 F.3d 891 (9th Cir. 2016).

291. *Id.* at 896, 907.

292. *Id.* at 896.

293. Under California law, plaintiffs attempting to assert claims that might be barred by First Amendment protections must first prove the lawsuit is not intended to deter speech under the anti-SLAPP (strategic lawsuit against public participation) laws. CAL. CIV. PROC. CODE § 425.16(b)(1) (West 2022).

294. *Sarver*, 813 F.3d at 905.

unflattering.[295] "The 101-year-old actress sued . . . claiming the series *Feud: Bette and Joan* makes her seem like a vulgar hypocrite and gossip."[296] The court again rejected such claims.

> Books, films, and television shows are "things" but are they "merchandise" or "products"?
>
> . . . .
>
> *Feud* is as constitutionally protected as was the film in *Sarver*, *The Hurt Locker*. As with that expressive work, *Feud* "is speech that is fully protected by the First Amendment, which safeguards the storytellers and artists who take the raw materials of life—including the stories of real individuals, ordinary or extraordinary—and transform them into art, be it articles, books, movies, or plays.[297]

These cases suggest a clear line between communicative works such as articles, books, movies, or plays entitled to First Amendment protection on one hand, and the advertisements, tchotchkes, and endorsements on the other.[298] The problem for Ginormaverse and video games more generally is that despite an unequivocal statement by the Supreme Court that video games are entitled to full First Amendment protection,[299] courts have been reluctant to see video games with the same level of free speech interests as books, movies, and plays.[300] Rather than simply finding these works to be categorically communicative, the courts have applied a balancing test.

In recent cases involving student athletes, courts found that the accurate reproduction of a virtual sports environment resulted in an unauthorized use of

---

295. De Havilland v. FX Networks, LLC, 230 Cal. Rptr. 3d 625 (Cal. Ct. App. 2018).

296. Ashley Cullins, *FX Wins Appellate Court "Feud" With Olivia de Havilland*, HOLLYWOOD REP. (Mar. 26, 2018), https://www.hollywoodreporter.com/business/business-news/fx-wins-appellate-court-feud-olivia-de-havilland-1097518/ [https://perma.cc/Z9CY-2X63].

297. *De Havilland*, 230 Cal. Rptr. 3d at 636, 638.

298. *Id.* at 636.

> Many of the cases in this area involve products and merchandise such as T-shirts and lithographs [Prod. v. Gary Saderup, Inc., 21 P.3d 797 (Cal. 2001)], greeting cards [Hilton v. Hallmark Cards 599 F.3d 894 (9th Cir. 2010)], and video games [Davis v. Elec. Arts, Inc. 775 F.3d 1172 (9th Cir. 2015]; [*In re* NCAA Student-Athlete Name & Likeness 724 F.3d 1268 (9th Cir. 2013)]; [Kirby v. Sega of Am., Inc. 144 Cal.App.4th 47, (2006)], or advertisements for products and merchandise. [*See*, *e.g.*, Newcombe v. Adolf Coors Co. 157 F.3d 686, 691-694 (9th Cir. 1998) [beer advertisement]; [Waits v. Frito-Lay, Inc. 978 F.2d 1093 (9th Cir. 1992)] [advertisement for SalsaRio Doritos]; Midler v. Ford Motor Co. 849 F.2d 460 (9th Cir. 1988) [advertisement for Ford Lincoln Mercury] . . . .

Id.

299. Brown v. Ent. Merch. Ass'n, 564 U.S. 786, 791 (2011).

300. *See* Hart v. Elec. Arts, Inc., 717 F.3d 141, 144–49 (3d Cir. 2013); *In re* NCAA Student-Athlete Name & Likeness Licensing Litig., 724 F.3d 1268, 1271 (9th Cir. 2013).

the athlete's name or likeness.[301] These courts struggled with the use of a transformative test, but neither court asked why a video game author would require greater rights than a broadcaster, newspaper, or filmmaker.[302]

The distinction will become critical to the way in which Ginormaverse looks to draft its ToS. The metaverse platform will undoubtedly require express permission of anyone seeking to create an avatar within the system. But this will not be enough. There will be events held within the system importing content from other news and media resources. Even if courts are eventually going to recognize that a press conference played in Ginormaverse should require no publicity rights, just as no television, radio, or print service requires these rights, the difference in treatment could lead to costly litigation and confusion.

In addition, if the law requires Ginormaverse to have expansive authority for use of publicity rights, then the contractual grant will be much broader. From a consumer protection standard, the goal would be to have the platform obtain only minimal rights, with the individual retaining all rights for exploitation of one's name, image, and likeness when used to actually endorse products or services, to sell goods, or to otherwise commercialize one's publicity rights. An actor or athlete will need to give the platform permission to recreate their image in order for that person to have an accurate avatar within the metaverse. But that initial grant should not include the right to sublicense it to other entities for purposes of commercialization. The ToS should be appropriately limited in scope.

The better understanding is that the use of one's name, image, or likeness within the metaverse is not an exploitation of publicity rights. Avatars presenting the news can use the names of individuals in their stories in precisely the same manner as can other news presenters. Storytellers can name-check celebrities in in-world content to the extent they can do so in current media.

In contrast, when a person or enterprise uses a person's name, image, or likeness to endorse a product or service, to create an advertisement, or to otherwise attempt to sell any goods or services, in that instance, the individual rights of publicity must be obtained as a condition of the usage. For example, assume a famous actor can be seen in a virtual world having coffee while sitting in an open plaza. That should not require any rights of publicity. If the public can walk up to that actor and ask her for store recommendations, then those endorsements should only be permitted if the actor has given permission in advance. If the public can link from the purse, shoes, or clothing on the avatar

301. *See, e.g.*, *Hart*, 717 F.3d at 170; *In re NCAA*, 724 F.3d at 1284.

302. *E.g.*, *Hart*, 717 F.3d at 169; *In re NCAA*, 724 F.3d at 1284.

to a store selling those items, then again, the vendors should be required to obtain express permission. The recommendations and endorsements transform the avatar's use into a commercial exploitation of the avatar owner's likeness. These uses of a person's name, image, and likeness are commercial in nature.

In addition to the rights of publicity, the FTC creates affirmative duties for product endorsements.[303] In 2021, the FTC significantly stepped up its enforcement against false endorsements, fake reviews, and similar consumer deceptions.[304] There is a commensurate harm to anyone who can provide endorsements for goods or services but finds that fake reports undermine the public value in those endorsements. As such, rights of publicity must be carefully protected in all instances where an actual endorsement is taking place, while providing traditional First Amendment protections when these commercial interests are not present.

F. Free Speech and ToS Restrictive Conditions

A related area has also received considerable attention. The commercial marketplace is strongly benefitted from truthful disclosure of information regarding products and services.[305] The Supreme Court has often recognized "the consumers' interest in the receipt of accurate information in the commercial market by prohibiting fraudulent and misleading advertising."[306] Given this fundamental public interest in accurate consumer information, it is unsurprising that there are ongoing concerns about efforts to include restrictions

---

303. *See* Federal Trade Commission Act, 15 U.S.C. § 45; Guides Concerning the Use of Endorsements and Testimonials in Advertising, 16 C.F.R. § 255 (2021).

304. *See* Press Release, FTC, FTC Puts Hundreds of Businesses on Notice about Fake Reviews and Other Misleading Endorsements (Oct. 13, 2021), https://www.ftc.gov/news-events/press-releases/2021/10/ftc-puts-hundreds-businesses-notice-about-fake-reviews-other [https://perma.cc/HG3L-XGVG]

> The rise of social media has blurred the line between authentic content and advertising, leading to an explosion in deceptive endorsements across the marketplace. Fake online reviews and other deceptive endorsements often tout products throughout the online world. Consequently, the FTC is now using its Penalty Offense Authority to remind advertisers of the law and deter them from breaking it. By sending a Notice of Penalty Offenses to more than 700 companies, the agency is placing them on notice they could incur significant civil penalties—up to $43,792 per violation—if they use endorsements in ways that run counter to prior FTC administrative cases.

Id.

305. *See* Va. Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc., 425 U.S. 748, 769–70 (1976); Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n, 447 U.S. 557, 562 (1980); 44 Liquormart, Inc. v. Rhode Island, 517 U.S. 484, 503 (1996); Sorrell v. IMS Health Inc., 564 U.S. 552, 577–78 (2011).

306. *44 Liquormart, Inc.*, 517 U.S. at 496.

on truthful product and service reviews in licensing agreements.[307] In 2021, a new association, Transparency in Cybersecurity, was formed to address contractual restrictions addressing general product assessments as well as identifying cybersecurity threats.[308] Transparency in Cybersecurity launched with a review of 200 EULAs. "Of this sampling, 42% of companies had clauses that in some fashion prohibit users from publicly disclosing assessments of their products. Public companies tended to be less transparent, with 53% featuring restrictions in their EULAs, compared to just 39% of private companies."[309]

The concern about contractual limits on truthful product information has been a concern since the shift to licensed software and goods expanded in the modern internet age.

> [Restrictive] clickwrap agreements, if upheld, violate the consumer's fundamental, rather than economic, rights. For example, a number of such agreements require users to waive their free speech rights by prohibiting them from engaging in public criticism of the developing company or its products, publishing benchmark results (an objective measure of a program's performance across differing hardware configuration), or even reviews.[310]

Although the concern over the public's right to truthful product information is not new, the potential for a monopolistic or oligopolistic ToS used to cover a person's entire professional and social life has far more sweeping effects than a similar provision in just a computer operating system or commercial website. To the extent Ginormaverse's ToS becomes universal, it serves to supplant positive law under an increasingly misplaced freedom to contract principle.

VI. LIMITATIONS ON THE GOVERNMENT: WARRANT REQUIREMENTS, THIRD PARTY DOCTRINE, AND THE POWER OF SUBPOENAS

Another area that may be significantly impacted by a universal metaverse is the extent to which personal privacy services are protected against

---

307. *See* Bradley Barth, *Silenced? Transparency Effort Looks to Squash Vendor Restrictions on Product Reviews by Users*, SC MEDIA (Aug. 11, 2021), https://www.scmagazine.com/feature/policy/silenced-transparency-effort-looks-to-squash-vendor-restrictions-on-product-reviews-by-users [https://perma.cc/L22Y-6MJQ].

308. *Id.*

309. *Id.*; s*ee also* Lydia Pallas Loren, *Slaying the Leather-Winged Demons in the Night: Reforming Copyright Owner Contracting with Clickwrap Misuse*, 30 OHIO N.U. L. REV. 495, 497 (2004); David R. Collins, *Shrinkwrap, Clickwrap, and Other Software License Agreements: Litigating a Digital Pig in a Poke in West Virginia*, 111 W. VA. L. REV. 531, 550 (2009).

310. Collins, *supra* note 309, at 550.

unwarranted government intrusions.[311] The government has always sought private information regarding suspected criminals as part of its law enforcement strategies, but with the "terrorist attacks of September 11, 2001, the impetus for the government to gather personal information has greatly increased."[312] Data has become an essential element in the war on terror.[313] As society has learned with the recent pandemic, data is also an essential element in the delivery of public health.[314] Some view this issue as an important civil rights and social justice issue[315] while others frame it in the civil liberties context.[316] The continuing publicity surrounding government officials' use of contact tracing and health outcomes highlights the significance of personal information and behavioral data. These data go well beyond one's personally identifiable information to include all aspects of an individual's activities, interactions, attitudes, and preferences.

The government is not necessarily just Big Brother. Although there are concerns about overwhelming access to personal information fueling a totalitarian state,[317] there are a myriad of smaller concerns about local law enforcement, municipal services, and voter manipulation that could all create social concerns if the government has unbridled access to individual and collective private information.

In the context of cell phones and vehicle tracking, the Supreme Court has adopted a series of significant decisions in favor of individual privacy.[318] These

---

311. *See* Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083 (2002).

312. *Id.* at 1084.

313. *Id.*

314. *See Public Health, Surveillance, and Human Rights Network. Surveillance and the "New Normal" of Covid-19: Public Health, Data, and Justice*. *New York*, SOC. SCI. RSCH. COUNS. (2021) https://covid19research.ssrc.org/public-health-surveillance-and-human-rights-network/report/ [https://perma.cc/N5PM-C2NJ].

315. *See* Angela P. Harris & Aysha Pamukcu, *The Civil Rights of Health: A New Approach to Challenging Structural Inequality*, 67 UCLA L. REV. 758, 804–05 (2020).

316. *See* Ronald Bayer, *The Continuing Tensions Between Individual Rights and Public Health: Talking Point on Public Health Versus Civil Liberties*, 8 EUR. MOLECULAR BIOLOGY ORG. REPS., no. 12, 2007, at 1099 https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2267241/ [https://perma.cc/ZW57-NH37].

317. Solove, *supra* note 311, at 1804–85 ("Inadequately constrained government information-gathering can lead to at least three types of harms. First, it can result in the slow creep toward a totalitarian state. Second, it can chill democratic activities and interfere with individual self-determination. Third, it can lead to the danger of harms arising in bureaucratic settings.").

318. *See* United States v. Jones, 565 U.S. 400, 404 (2012) (warrant was required when police placed tracking device on suspect's car); Riley v. California, 573 U.S. 373, 387 (2014) (the "immense storage capacity" of cell phones require that police obtain a warrant before conducting a general search

changes, however, have been incremental in nature and may not keep pace with the public's shift away from personal records to data stored by third parties and managed outside the control by most citizens. As the metaverse further accelerates the use of cloud-based data storage and increases the location of proprietary information outside the home, statutory and constitutional protections against government collection and misuse of data become increasingly important.

The Fourth Amendment applies to protect an individual from an unauthorized search and seizure of "persons, houses, papers, and effects."[319] "The Fourth Amendment strikes a balance between liberty and social order—two concepts which stand on opposite sides of an ideological teeter-totter."[320] The Supreme Court has had to reconcile this balance as technology has evolved. Nearly a century ago, in *Olmstead v. United States*,[321] the Court faced the intrusion of the modern age of telephones, radios, and wired communications. The Court refused to extend to telegraph and telephone messages the protections afforded to the mail because the mail service was a government monopoly.[322]

Under this logic, outside the home, the Fourth Amendment only extended to the government's monopolistic control over one's communications. Information in the private sphere was not subject to any extension of the Fourth Amendment. Unlike "the unlawful rifling by a government agent of a sealed letter," the telephone wires were not under government control.[323] As such, "[t]here was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[324]

---

in the contents of a phone); Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) (requiring a warrant for a search of cell-site location information (CSLI)).

319. U.S. CONST. amend. IV (The "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.").

320. Tricia A. Martino, *Fear of Change:* Carpenter v. United States *and Third-Party Doctrine*, 58 DUQ. L. REV. 353, 356 (2020); *see also* James J. Tomkovicz, *Technology and the Threshold of the Fourth Amendment: A Tale of Two Futures*, 72 MISS. L.J. 317, 324–25 (2002).

321. 277 U.S. 438, 464 (1928).

322. *Id.*

323. *Id.* at 464–65.

324. *Id.* at 464.

Olmstead was eventually rejected by statute[325] and later overturned by *Berger v. State of New York*[326] and *Katz v. United States*.[327] Significantly, *Katz* rejected *Olmstead's* limited view of the Fourth Amendment.[328] The Court extended Fourth Amendment protections beyond places to people.[329] As part of this expansion, the Court reframed the Fourth Amendment as protecting an individual's reasonable expectation of privacy.[330] As the Court recently summarized, "[w]hen an individual 'seeks to preserve something as private,' and his expectation of privacy is 'one that society is prepared to recognize as reasonable,' we have held that official intrusion into that private sphere generally qualifies as a search and requires a warrant supported by probable cause."[331]

Over time, the list of activities protected by the warrant requirement has been expanded. In 2014, the Court used traditional trespass doctrine to find that sneaking onto a person's driveway without a warrant to place a GPS tracking device constituted an unwarranted, unlawful search.[332] Justice Sotomayor, in concurrence, suggested that the real threat is the extended, low-cost volume of information that can be made subject to government search. As she explained, "I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[333] The Court took those concerns seriously. Two years later, the Supreme Court recognized that the significant amount of personal information on a person's cell phone requires that a cell phone be protected by a search warrant requirement, even when seized as part of a lawful arrest.[334] In the third Supreme

325. *See* GINA STEVENS & CHARLES DOYLE, CONG. RSCH. SERV., PRIVACY: AN OVERVIEW OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING 2 (2012) ("By the time of the landmark Supreme Court decision in Olmstead, however, at least forty-one of the forty-eight states had banned wiretapping or forbidden telephone and telegraph employees and officers from disclosing the content of telephone or telegraph messages or both.").

326. 388 U.S. 41, 63–64 (1967).

327. 389 U.S. 347, 353 (1967).

328. *Id.* at 353.

329. *Id.* at 351 ("[T]he Fourth Amendment protects people, not places.").

330. *Id*. at 361 (Harlan, J., concurring) ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.' ").

331. Carpenter v. United States, 138 S. Ct. 2206, 2213 (2018) (quoting Smith v. Maryland, 442 U.S. 735, 740 (1979)).

332. United States v. Jones, 565 U.S. 400, 405 (2012).

333. *Id.* at 416 (Sotomayor, J., concurring).

334. Riley v. California, 573 U.S. 373, 387 (2014).

Court decision on technology searches, the Court again required a search warrant. In this case, it was for cell site location information (CLSI).[335]

Although the Supreme Court decided that the request for CLSI required a warrant, it tried to provide very incremental guidance regarding the warrant requirements for searches of third party records.[336] The doctrinal challenge is that, historically, records held by third parties did not require a search warrant, and as a result, the government could obtain financial records, repair records, purchase histories, and many other forms of behavioral records without any need to establish probable cause or specify with particularity the items to be searched.[337]

In an important pair of decisions during the 1970s, the Supreme Court created the third-party doctrine.[338] The doctrine developed in the context of a tax evasion case, where "the Government subpoenaed [defendant Mitch Miller's financial records to show his income from an unlicensed still,] seeking several months of canceled checks, deposit slips, and monthly statements."[339] There, at least some of the records were "not confidential communications but negotiable instruments to be used in commercial transactions."[340] Other records, however, were turned over to the bank for the purpose of the bank's use on behalf of the defendant, but they were still records out of the defendant's

---

335. *Carpenter*, 138 S. Ct. 2206 at 2211–12.

> Each time the phone connects to a cell site, it generates a time-stamped record known as cell-site location information (CSLI). The precision of this information depends on the size of the geographic area covered by the cell site. . . .
>
> Wireless carriers collect and store CSLI for their own business purposes, including finding weak spots in their network and applying "roaming" charges when another carrier routes data through their cell sites. . . . [I]n recent years phone companies have also collected location information from the transmission of text messages and routine data connections. Accordingly, modern cell phones generate increasingly vast amounts of increasingly precise CSLI.

Id.

336. *Id*. at 2214–15 ("This sort of digital data—personal location information maintained by a third party—does not fit neatly under existing precedents. Instead, requests for cell-site records lie at the intersection of two lines of cases, both of which inform our understanding of the privacy interests at stake.").

337. *See* Marron v. United States, 275 U.S. 192, 196 (1927) ("The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.").

338. United States v. Miller, 425 U.S. 435, 437 (1976) (ruling that the government obtainment of bank records was not a Fourth Amendment search); Smith v. Maryland, 442 U.S. 735, 745–46 (1979) (ruling that the government's use of a pen register was not a Fourth Amendment search).

339. *Carpenter*, 138 S. Ct. at 2216 (citing *Miller*, 425 U.S. at 438, 442).

340. *Miller*, 425 U.S. at 442.

control.[341] The Court did not see a difference between records provided to the public and records intended to be treated confidentially between the parties.[342] "The Court thus concluded that Miller had 'take[n] the risk, in revealing his affairs to another, that the information [would] be conveyed by that person to the Government.' "[343]

In *Smith v. Maryland*, the Court expanded the third-party doctrine to all records, without regard to the party's knowledge that the records were being kept or the purpose to which they were being put.[344] The Court permitted the "pen register" information providing telephone records regarding who was making phone calls into and out of various telephone numbers.[345] Although the government would be required to have a warrant to listen into the calls, it could obtain the records from the phone company with a simple subpoena.[346]

In her concurrence in *Jones*, Justice Sotomayor suggested that the third-party doctrine might be inappropriate for the modern era of historical data searches and ubiquitous tracking. "[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," she explained.[347] "This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[348]

Without addressing the continuing application of the third-party doctrine in established cases, *Carpenter* declined to extend the third-party doctrine to CSLI searches.[349] At the same time, however, the decision was intended to be narrow and incremental.

> Our decision today is a narrow one. We do not express a view on matters not before us: real-time CSLI or "tower dumps" (a download of information on all the devices that connected to a particular cell site during a particular interval). We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information.

341. *Id.* at 437–38.
342. *Id.* at 435.
343. *Carpenter*, 138 S. Ct. at 2216 (quoting *Miller*, 425 U.S. at 443).
344. Smith v. Maryland, 442 U.S. 735, 744–45 (1979).
345. *Id.* at 745–46.
346. *Id.*
347. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J. concurring).
348. *Id.*
349. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

> Further, our opinion does not consider other collection techniques involving foreign affairs or national security. As Justice Frankfurter noted when considering new innovations in airplanes and radios, the Court must tread carefully in such cases, to ensure that we do not "embarrass the future."[350]

As 5G expands bandwidth, the potential for virtual and augmented reality to become mobile adds another dimension to the regulation of the metaverse. Lower courts have split on the issue of whether tower dumps require warrants.[351] If online worlds include GPS or other location data in the way *Ingress* and *Pokémon Go* take advantage of location information, then law enforcement (and civil litigators) will have a significant new tool to track the public's movement.

Beyond the physical intrusion into one's home or one's movements, however, the law continues to embrace the third-party doctrine enthusiastically. "Investigators have a handful of tools to compel the disclosure of electronic data, and a subpoena is the easiest to obtain because the government is not required to provide cause for obtaining the information. Subpoenas don't require a judge to issue them."[352]

Since the Fourth Amendment does not provide a warrant requirement for most third-party records, Congress passed federal legislation to supplement the constitutional right. Shortly after *Katz* extended Fourth Amendment protections, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968.[353] Title III of the statute is known as the "Wiretap Act," which has been subsequently expanded to also include the Stored Communications Act.[354] The Wiretap Act prohibits the interception of both oral and wire communications, but also provides a mechanism for seeking a court order to issue a wiretap or electronic surveillance.[355]

---

350. *Id.* at 2220 (quoting Northwest Airlines v. Minnesota, 322 U.S. 292, 300 (1944)).

351. *See* ANNE TOOMEY MCKENNA & CLIFFORD S. FISHMAN, WIRETAPPING AND EAVESDROPPING § 28:8 (2021); *In re* Cell Tower Records Under 18 U.S.C. § 2703(D), 90 F. Supp. 3d 673, 675 (S.D. Tex. 2015); Matter of Search of Info. Stored at Premises Controlled by Google, 481 F. Supp. 3d 730, 738 (N.D. Ill. 2020); United States v. Adkinson, 916 F.3d 605, 608 (7th Cir. 2019), *cert. denied,* 139 S. Ct. 2762 (2019).

352. Jay Greene, *Tech Giants Have to Hand Over your Data When Federal Investigators Ask. Here's Why*, WASH. POST (June 15, 2021), https://www.washingtonpost.com/technology/2021/06/15/faq-data-subpoena-investigation/ [https://perma.cc/4WP7-TKNW].

353. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, 82 Stat. 197 (codified at 18 U.S.C. § 2510).

354. 18 U.S.C. §§ 2701–12.

355. *Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, U.S. DEP'T OF JUST.:BUREAU OF JUST. ASSISTANCE, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1284 [https://perma.cc/5E4E-D7AM].

The architecture of the Stored Communications Act (SCA) is based on 1986 legislation and has evolved from an understanding of how email communications are transferred and stored.[356] As a result, the SCA covers "remote computing services" (RCS), which were third-party data processing centers and providers or electronic communications services (ECS), which were precursors to Internet Service Providers (ISPs) that sent and received customer information such as emails.[357] Over time, as the service providers integrated the functions, the distinction between ECS and RCS focused on the status of the record being sought by the government rather than the contractual relationship between the customer and the service.

ECS includes live communications, digital wiretaps, and files such as unopened emails. Under the SCA, any file that falls into this category requires a traditional search warrant to be accessed by the government, unless the access is available to it under an exception to the search warrant requirement.[358]

One possible exception to the search warrant requirement is consent. The customer's consent may be circuitous. An ISP may prohibit illegal content such as gambling, drug sales, child pornography, or obscenity from being stored within the ISP's system. The ISP may further reserve the right to disclose such materials that are illegal and in violation of the ISP's terms of service.[359] Under such a ToS, the result would be that the customer has essentially consented to the ISP turning over the incriminating, illegal files directly to law enforcement.[360] The potential for law enforcement is significant, particularly if

---

356. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending it*, 72 GEO. WASH. L. REV. 1208, 1213 (2004).

357. *Id.* at 1214.

358. See Claudia G. Catalano, Annotation, Criminal Defendant's Rights Under Stored Communications Act, 18 U.S.C.A. §§ 2701 et seq., 11 A.L.R. Fed. 3d Art. 1 § 2 (2016) ("A warrant 'issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures) by a court of competent jurisdiction' is required to obtain content from an ECS in electronic storage for 180 days or less.").

359. *See, e.g.*, Laurie Sullivan, *Google To Scan Files In Its Cloud Services For Illegal, Harmful Content*, MEDIAPOST (Dec. 20, 2021), https://www.mediapost.com/publications/article/369579/google-to-scan-files-in-its-cloud-services-for-ill.html [https://perma.cc/N5PY-TSG2] ("A Google policy . . . focuses on Google's drive cloud-storage service, restricting access to files that violate company guidelines and terms of use. Google, using algorithms that scan the content, will keep a closer eye on harmful content ranging from cybercrime offenses to the protection of copyright law and child sexual abuse.").

360. *See, e.g.*, United States v. Kovacs, No. 3:20-CR-51, 2021 WL 3562920, at *8 (S.D. Ohio Aug. 11, 2021) ("Dropbox initially sent a complaint into NCMEC regarding Defendant's activities in 2017, MeWe's September 2019 report—stating that Defendant's IP address was being used to log into a MeWe account containing suspected child pornography—provides a temporal reference to the illegal activity at the time the search warrant issued."); Dylan Carroll, *Child Pornography Statutes and the*

the government is both providing contracts to major metaverse enterprises and asking those enterprises to have expansive rights to protect the public under the ToS.

For stored communications, the government also has the ability to obtain records with something less than a search warrant. A subpoena is sufficient to obtain "(A) name; (B) address; (C) local and long distance telephone connection records . . . (D) length of service (including start date) and types of service utilized; (E) . . . subscriber number or identity . . . and (F) means and source of payment for such service (including any credit card or bank account number) . . . ."[361] Although there are additional steps between a subpoena and the transactional logs, the bulk of customer records can be obtained using what is known as a 2703(d) court order. Here, the judge or magistrate can issue an order to provide records, so long as the government has established "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation."[362]

The specificity of the 2703(d) order is substantially less than that of a search warrant but still stronger than a mere subpoena. These orders collect a great deal of data.

> In the cases that have been determined thus far, courts have concluded that applications for an e-mail or a text message, posting to social networking service; cell site location information, generally; and historical or prospective cell site location data have all met the "specific and articulable facts" standard. Most court have found that requests for subscriber record or information met the standard, but one court found the application to be deficient in the case before it.[363]

Cloud: Updating Judicial Interpretations for New Technologies, 57 HOUS. L. Rev. 727, 736 n.36 (2020) ("[C]ompanies like Dropbox actively work with law enforcement to find and expose users who use the service for possession of child pornography.") (citing Kate Knibbs, *Dropbox Refuses to Explain Its Mysterious Child Porn Detection Software*, GIZMODO (Aug. 12, 2015), https://gizmodo.com/dropbox-refuses-to-explain-its-mysterious-child-porn-de-1722573363 [https://perma.cc/HH8A-GWGG] ("Looking at its Terms of Service, Dropbox states that it can search through your files to see if they comply with its ToS and Acceptable Use Policy. The company can look for way more than just vile child exploitation images—it can search for hate speech, any illegal porn, and anything that infringes on someone else's privacy.")).

361. H. MARSHALL JARRETT, MICHAEL W. BAILIE, ED HAGEN & NATHAN JUDISH, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 128 (2002) (citing 18 U.S.C. § 2703(c)(2)).

362. 18 U.S.C.A. § 2703(d); *see* Catalano, *supra* note 358, at 11.

363. Catalano, *supra* note 358, at 14 (collecting cases).

The broad scope of the 2703(d) court orders and the ability to expand further in situations where the ToS grants the ISP rights to review stored records will create the potential to undermine public protection from government surveillance. These fears will undoubtedly reinforce the efforts of DAO organizers to promote decentralized metaverse systems that add friction to easy governmental surveillance. These concerns may be even greater in other jurisdictions where restrictions on government access to personal information are subject to even less protection.

Concerns over privacy protections from the government will lead to some architectural choices in the metaverse. Privacy advocates will certainly promote use of encryption technologies that reduce the ability of ISPs and other third parties from accessing user information. Privacy, data security, and bandwidth considerations all suggest that the metaverse architecture leans more heavily on local storage and processing power. This approach will make the individual's smart cell phone an even more important part of their user experience, but the aggregate storage and processing power could significantly benefit the exploitation of the technologies. Phones with peripherals (such as keyboards, monitors, and remote printing) could finally eliminate the duplicative capacity of laptops and desktops, furthering a consolidation into metaverse technologies.

The movement into the metaverse could also trigger further expansion of Fourth Amendment jurisprudence into the virtual space. The Supreme Court has demonstrated its reluctance to rely on the third-party doctrine in ways that ignore the practical changes technology have had on the public's lifestyles. Perhaps, as the metaverse becomes widely adopted, the Court will recognize that a virtual home is as much as a castle as a house made out of brick and mortar, providing the same level of protection that the Court has already extended to the smartphone. If the Supreme Court someday recognizes the centrality of the metaverse, then the era of Web3 and the metaverse will have truly arrived.

VII. CONCLUSION

Some version of the metaverse is inevitable. The growth of Roblox, popularity of Bitmoji, and a generation of online worlds have intersected with the economic clout of cryptocurrencies and the potential of nonfungible tokens to usher in a new set of use cases that will evolve to make Web3 as profoundly different from the current internet as the current environment is different from America Online and the early internet portals. Even in the domestic marketplace, the nature of new transactions will trigger a wave of updated regulation, business model innovation, and wealth transfer that will leave many wondering how we got here.

Fortunately, the fundamentals for business have not changed. Relationships are governed by contract law, and contract law is interpreted through a longstanding common law tradition. Securities laws and antitrust considerations have been raised in each generation where new business models have sought to upend the historical way of doing business. Lessons from the Web 2.0 experience will likely leave both consumers and regulators of start-ups to seek safe harbors intended to let the new companies develop. Those Web 2.0 companies have grown to dominate the global economy, and the public appetite for sweetheart deals has likely passed.

The leaders of the Web3 movement are decidedly focused on reclaiming the property rights lost to Web 2.0. Using NFTs to enforce property and direct user control to discourage corporate overreach, the Web3 movement has the potential to rectify the imbalances of the past. At the moment, many of the promises may be loose predictions, but hopefully, this roadmap will help those building, investing, and regulating in these future technologies see where an optimal mix of private contracting, innovation, and government regulation. Since the movement will bring even more of our daily lives onto the internet, courts and regulators must also anticipate how that will affect our constitutional rights and civil liberties.

Two things are certain. First, this future that is already here will look quite different in the decades to come. Second, the metaverse will be much more than just a game. The rest has yet to be written.