Yale Journal of Law & Technology
Volume 27, Issue 1

Everything New is Old Again: The Coming Metaverse, Platforms as Premises, and Addressing Harms that Occur Behind the Veil of Scale

Lara Putnam* **& Jena Martin****

Increasingly, social media companies have engaged in the creation, development, and deployment of "worlds" within a virtual reality setting, leading to significant interactions among users within these engineered spaces. However, this expansion has also been accompanied by harms. While some harms are unique to immersive reality technology, many mirror harms that occur in the analog environment, including fraud, theft, verbal abuse, and child sexual exploitation. Others replicate harms that have already exploded in non-immersive online spaces, including image-based sexual exploitation, cyberstalking, and invasion of privacy. Unfortunately, the architecture and infrastructure of these spaces has created what we coin here to be a "veil of scale"—behind which bad actors are able to hide, and through which criminal and civil actions are systemically unable to reach. Even when existing statutes are, in theory, fully applicable to individual bad actors who commit harms within virtual settings, our current regulation and enforcement infrastructure offers few options for redress when the person who commits the harm is anonymous and ephemeral. Moreover, because of Section 230 of the Communications Decency Act, which has been consistently held to limit social media platforms' liability for third-party "content," plaintiffs who attempt to make themselves whole by suing the platforms themselves have

* UCIS Research Professor in the Department of History at the University of Pittsburgh and the co-lead of the Southwest PA Civic Resilience Initiative at the University's Institute for Cyber Law, Policy, and Security.
** Professor and Katherine A. Ryan Chair for Global and International Law, St. Mary's University. This Article was supported, in part, by St. Mary's Faculty Support Grant. The authors would like to thank the following people for their insights, support, and contributions: Cody Corliss, Amy Cyphert, Renick Darnell-Martin, Adam MacLeod, Michael Madison, Caroline Osborne, and Kirsha Trychta. All errors are our own.

routinely been thwarted by courts.

In this Article, we make the case for using premises liability doctrine within the metaverse to address these harms and hold platform companies accountable. Specifically, by using this doctrine to hold corporations liable for harms within their engineered venues, platforms would be incentivized to use their superior knowledge of ongoing risks within their properties to prevent harm to others—just as premises law has done with regard to physical space for centuries. The premises framework provides a path of redress for victims of foreseeable, preventable, and egregious harm, while also recognizing that not all harms are preventable, and not all precautions are reasonable. As we face emerging harms facilitated by a new, engineered space of interaction, premises liability offers a familiar legal paradigm that (1) has sound jurisprudential foundations, (2) is well-aligned, for concrete technological reasons, with dilemmas of place-built risk and third-party harms, and therefore (3) can be taken with minimal adjustments and applied to real-world harms effectuated via the metaverse.

Article Contents

Introduction

> *The Metaverse has now become a place where you can get killed. Or at least have your brain reamed out to the point where you might as well be dead. . . . It serves them right, he realizes now. They made the place too vulnerable. They figured that the worst thing that could happen was that a virus might get transferred into your computer and force you to ungoggle and reboot your system. . . . Therefore, the Metaverse is wide open and undefended. . . . Anyone can go in and do anything that they want to. There are no cops. You can't defend yourself, you can't chase the bad people.*[1]

Up until a few years ago, to the extent that science fiction writer Neal Stephenson's 1992 vision of an online, immersive, interactive "metaverse" was coming true, it seemed to be doing so mainly in the form of video games.[2] As such, virtual reality seemed like something that legal thinkers could treat as a side curiosity, less urgent or central than the many other new vectors for profit and harm enabled by the internet.[3] But then

---

[1] NEAL STEPHENSON, SNOW CRASH 418 (1992).

[2] For a discussion of the early virtual reality spaces as gaming gatherings, see Simone Pathe, *Virtual Reality's Early Adopters Worry What Mainstream Usage Will Look Like in the Facebook Era*, PBS (Mar. 26, 2014) https://www.pbs.org/newshour/nation/virtual-realitys-early-adopters-worry-what-mainstream-usage-will-look-like-in-the-facebook-era [https://perma.cc/2YLK-YCHP] (noting how all of then-Facebook's initial sales of Oculus headsets were to gamers). One example of the early gaming atmosphere surrounding virtual reality (VR) was Epic Games championing of its game Fortnite and its "unique potential" to interact with the metaverse. *See* Matthew Ball, *Fortnite is the Future, but Probably Not for the Reasons You Think*, MATTHEWBALL.CO (Feb. 5, 2019), https://www.matthewball.co/all/fornite [https://perma.cc/Z7BJ-7C9P].

[3] *E.g.*, Orin S. Kerr, *Criminal Law in Virtual Worlds*, 2008 U. CHI. L. F. 415 (2008); Jack Balkin, *Virtual Liberty: Freedom To Design And Freedom To*

two things happened, nearly simultaneously. First, machine learning algorithms and artificial intelligence (AI) hit new levels of effectiveness,[4] such that the real-time rendition of visually detailed and smoothly interactive three-dimensional worlds became cheaper and easier.[5] Second, the COVID-19 pandemic pushed unprecedented amounts of social, professional, and retail interactions online, as companies and individuals worldwide responded to restrictions on mobility and fears of face-to-face contagion.[6]

The pandemic push demonstrated that huge profits might be reaped by companies ready to meet consumer demand for virtual interaction in times of public health emergencies—or maybe even at any time. Meanwhile, as "Zoom meetings" and "work from home" boomed and travel and event spending evaporated, corporate leaders saw proof-of-concept for the cost savings that might be generated by enterprise uses of virtual interaction. The technology giants best positioned to leverage their existing offerings and talent to move into this emerging market noticed.[7] And investors noticed as well.[8]

In October 2021, the company formally known as Facebook announced its entry into the world of augmented reality by

---

Play In Virtual Worlds, 90 VA. L. REV. 2043, 2045 (2004); Dan Hunter & Greg Lastowka, *Virtual Crimes*, 49 N.Y.L. SCH. L. REV. 293, 294 (2004-05); Bettina M. Chin, *Regulating Your Second Life: Defamation in Virtual Worlds*, 72 BROOK. L. REV. 1303 (2007); Sara M. Smyth, *Back to the Future: In Search of an Understanding of Crime and Punishment in Second Life*, 36 RUTGERS COMP. & TECH. L.J. 18 (2009).

[4] In fact, the first law review article to discuss the legal implications of generative artificial intelligence (AI)—arguably AI's most significant shift into popular culture—was not written until 2021. *See generally*, Amy Cyphert, *A Human Being Wrote This Law Review Article: GPT-3 and the Practice of Law*, 55 U.C. DAVIS L. REV. 401 (2021) (discussing the legal implications of ChatGPT's precursor, GPT-3, and its underlying technology).

[5] Kelly Ommundsen & Jaci Eisenberg, *AI is Shaping the Metaverse - but How? Industry Experts Explain*, WORLD ECON. F. (May 9, 2023), https://www.weforum.org/agenda/2023/05/generative-ai-and-how-can-it-shape-the-metaverse-industry-experts-explain/ [https://perma.cc/X6D7-5YUG].

[6] *See* discussion *infra*, Section I.C.

[7] *Id.*

[8] *Id.*

changing its name to Meta.[9] Yet Meta had already been planning this investment—seven years prior to the name change, the company had acquired Oculus, a successful developer of virtual reality headsets, for $2 billion in cash and stock.[10] Since then, Meta has spent $36 billion on metaverse initiatives, despite their unprofitability.[11] The aggressive development continued even as Meta made significant layoffs throughout 2023,[12] and analysts voiced concerns over the

---

[9] Benjamin Curry & Michael Adams, *Facebook Changes Ticker To META From FB*, FORBES ADVISOR (Sep. 22, 2023), https://www.forbes.com/advisor/investing/facebook-ticker-change-meta-fb/#:~:text=Facebook%20parent%20company%20Meta%20Platforms, October%202021%2C%20is%20effective%20today [https://perma.cc/6XMS-RGKM]. Perhaps not coincidentally, the name-change announcement also came shortly after *The Wall Street Journal* began publishing its investigative reporting series into the company's internal research and its "possible negative impacts on the day-to-day lives of a broad swath of users." Georgia Wells, Deepa Seetharaman & Jeff Horwitz, *Is Facebook Bad for You? It Is for About 360 Million Users, Company Surveys Suggest*, WALL ST. J. (Nov. 5, 2021), https://www.wsj.com/articles/facebook-bad-for-you-360-million-users-say-yes-company-documents-facebook-files-11636124681?mod=article_inline; *see also*, *The Facebook Files: A Wall Street Journal Investigation*, WALL ST. J., https://www.wsj.com/articles/the-facebook-files-11631713039. Many of the documents used in the reporting came from a former Facebook employee and whistleblower, Frances Haugen, who collected an unprecedented amount of damaging information on the company and its marketing and post-amplification practices. For a fuller discussion of the scandal and its implications on potential social media liability, *see* Amy Cyphert & Jena Martin, *"A Change is Gonna Come:" Developing a Liability Framework for Social Media Algorithmic Amplification*, 13 U.C. IRVINE L. REV. 155, 160-65 (2022).

[10] Erica Sweeney, *Oculus: Virtual Reality Company's Complete History and Device Development*, BUS. INSIDER (Oct. 27, 2023), https://www.businessinsider.com/what-is-oculus#:~:text=initiative%20for%20Meta.-,Oculus%20was%20a%20virtual%20reality%20company%20founded%20by%20Palmer%20Luckey,later%20rebranded%20as%20Meta%20Quest [https://perma.cc/TZU6-QKTK].

[11] *Id.*

[12] Naomi Nix, *After Laying Off Thousands, Meta Expects to Add Jobs Next Year*, WASH. POST (Oct. 25, 2023), https://www.washingtonpost.com/technology/2023/10/25/meta-hires-2024-layoffs/.

company's ability to retain users of their virtual reality products.[13] Meta has continued to invest in the infrastructure that has come to be known as the metaverse,[14] and others have done likewise.[15]

---

[13] Ben Lang, *Meta Has Sold Nearly 20 Million Quest Headsets, but Retention Struggles Remain*, ROADTOVR (Mar. 1, 2023), https://www.roadtovr.com/quest-sales-20-million-retention-struggles/ [https://perma.cc/R92S-AZUD].

[14] The term "metaverse" was first used in Neal Stephenson's 1992 novel *Snow Crash*. *See generally*, STEPHENSON, *supra* note 1. Many have hailed Stephenson's book as a prophetic voice regarding the virtual reality space. *See* Tom Huddelston, Jr., *The 29-Year-Old Book Predicted the 'Metaverse'—and Some of Facebook's Plans are Eerily Similar*, CNBC (Nov. 3, 2021), https://www.cnbc.com/2021/11/03/how-the-1992-sci-fi-novel-snow-crash-predicted-facebooks-metaverse.html#:~:text=Author%20Neal%20Stephenson%20coined%20the,based%20successor%20to%20the%20internet [https://perma.cc/WJ7D-WZMP]. Since its resurgence in popular culture, the term metaverse has been used interchangeably to connote such environments as (1) 3D immersive realities and (2) company-built individual "worlds" that generally uses those 3D realities. At this point, it is unclear whether there will be extensive crossover between each corporation's platforms. We use the term metaverse here to connote all corporate created communal environments that use immersive technology as their primary interface. *See* discussion, *infra*, Section I.A.

[15] *See* Eze Vidra, *The Top 10 Companies Investing Billions in the Metaverse*, VC CAFÉ (Aug. 2, 2022), https://www.vccafe.com/2022/08/02/the-top-10-companies-investing-billions-in-the-metaverse/ [https://perma.cc/4VZP-5MGX]. In addition to companies that have invested in the metaverse's infrastructure, other companies are spending significant funds developing within that infrastructure. *See* Aaron Drapkin, *Metaverse Companies: Who's Involved and Who's Investing in 2023*, TECH.CO (Mar. 21, 2023), https://tech.co/news/metaverse-companies-whos-involved-whos-investing [https://perma.cc/C8DV-RKAL] (discussing companies involved in development, including such corporations as Nike, Walmart, and Adidas). For a discussion of the ways in which the operations of more traditional "bricks and mortar" companies are intersecting with this environment see discussion *infra*, Part II. Indeed, Stephenson, the science fiction author behind *Snow Crash* (as discussed in *supra* note 1) is now taking part in its development. *See* Theo Zenou, *A Novel Predicted the Metaverse (and Hyperinflation) 30 Years Ago*, WASH. POST (June 30, 2022) (stating "thirty years after anticipating the future, Stephenson now intends to shape it. Along with Bitcoin Foundation co-founder Peter Vessenes, he recently

These trends together occasioned a "virtual land rush"[16] into the new, largely unregulated frontiers within the metaverse.[17] Companies, including many staid, big-name corporations that traditionally operated in the "real" or "analog" world, now offer their services within this new space and take advantage of the growing accessibility of virtual payment systems that facilitate commercial transactions within it.[18] And just as with the historical Wild West, this expansion has been accompanied by harms.[19]

The ease of holding corporations liable for torts that occur on their platforms is dependent on how they use the metaverse. When corporate actors use the metaverse as a glorified showroom or virtual office, novel harms may occur, but the lines of responsibility and legal redress will be straightforward. For instance, if a corporation demonstrates a product in the metaverse that turns out to malfunction in real life, traditional legal reasoning will link tortfeasor to tort and hold them accountable. Because the "tortfeasor" in that instance would be easily identifiable, plaintiffs would be able to gather evidence regarding whether that company acted negligently. However, the bulk of investment in the metaverse does not take this form of fixed and visible sellers building showrooms for which they are solely responsible. Rather, it is coming instead from social media companies—Meta, first and foremost—and from interactive gaming platforms that encourage the proliferation of ephemeral user-to-user

---

launched Lamina1, a start-up that will use blockchain technology to build an "open metaverse"—one that's "open-source and decentralized"), https://www.washingtonpost.com/history/2022/06/30/snow-crash-neal-stephenson-metaverse/.

[16] Musadiq Bidar & Dan Patterson, *Virtual Land Rush is Driving Up the Cost of Space in the Metaverse*, CBS NEWS (May 6, 2022), https://www.cbsnews.com/news/metaverse-real-estate-companies-land-rush/ [https://perma.cc/745X-894L] (stating that "more than 200 consumer-facing brands, including Gucci, Atari, Wari Music Group and HSBC, have already purchased virtual land in the metaverse").

[17] Drapkin, *supra* note 15.

[18] Bidar & Patterson, *supra* note 16.

[19] For a discussion on phenomena obscured by mythic versions of America's "Wild West," see generally, ALAINA E. ROBERTS, I'VE BEEN HERE ALL THE WHILE: BLACK FREEDOM ON NATIVE LAND (2021).

interactions that, as we discuss below, our current statutory frameworks cannot adequately address. Moreover, the business model of social media companies, and of some of the most successful immersive gaming platforms, like Roblox, relies specifically on this decentralized instance-building and the scaling force of frictionless and anonymous account formation. Systematically, then, the behemoths at the forefront of metaverse expansion expect to drive engagement and profits through user-generated content and interaction.

Given this profit scheme, jurists may assume that Section 230 of the Communications Decency Act of 1996 renders metaverse platforms prima facie untouchable:[20] Section 230 provides a broad immunity shield to "interactive computer service providers," who, under this law, cannot be "treated as publishers" of material generated by other "content providers."[21] Legislators may likewise assume Section 230's shield prevents accountability here, and take this as further reason to rewrite or repeal Section 230 altogether,[22] removing a pillar that has protected content moderation and speech on the internet.[23] Eschewing that false forced choice, this Article

---

[20] As we consider more comprehensively in Section I.B, *infra*, the legislation, which was passed at the dawn of the internet was, according to the Department of Justice, meant to "nurture emerging internet businesses while also incentivizing them to regulate harmful online content." *Department of Justice's Review of Section 230 of the Communications Decency Act of 1996*, DEP'T OF JUST. (2020), https://www.justice.gov/archives/ag/department-justice-s-review-section-230-communications-decency-act-1996#:~:text=The%20statute%20was%20meant%20to,Section%20230%2C%20could%20have%20predicted [https://perma.cc/FY9F-NFMZ].

[21] *See* discussion *infra* Section I.B.

[22] Rosie Moss, *The Legal Framework Before the Supreme Court*, NAT'L ASS'N OF ATT'YS GEN. (July 21, 2023) (stating that "in the past two years, there have been dozens of legislative proposals aimed at reforming Section 230. While some legislators have called for repealing Section 230 entirely, others have suggested reforms, such as establishing carve-outs for larger online companies or for certain types of content, requiring online platforms to remove certain content upon receiving notice that such content is unlawful, and adding exemptions for state criminal law or expanding federal criminal laws.").

[23] *See generally*, Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33 (2019).

argues that the well-developed jurisprudence of premises liability offers a way forward that is both efficient and normatively justified, all while conforming to Section 230's black letter law. Using a premises liability framework, jurists can hold those who create engineered virtual spaces responsible for predictable and repeated third-party harms that occur there, when and only when these harms surmount high thresholds.

What kind of harms occur in the metaverse? While some harms in the metaverse are unique to immersive reality ("IR") technology,[24] many others mirror harms that occur in the analog environment—including theft, bullying, sexual harassment, and child sexual exploitation. Others replicate the natively digital harms that have exploded in non-immersive online spaces as a result of the combination of smartphones and social media, including image-based sexual exploitation, cyberstalking, and digital invasion of privacy.[25]

Writing fifteen years ago, Orin Kerr argued that:

> Virtual worlds at bottom are computer games, and games are artificial structures better regulated by game administrators than federal or state governments. The best punishment for a violation of a game comes from the game itself. . . . It is only when harms go outside the game that the criminal law should be potentially available to remedy wrongs not redressable elsewhere.[26]

In the pages that follow, we argue that acts within the

---

[24] For some early scholarship on the metaverse and its harms, see Yogesh K. Dwivedi et al., *Exploring the Darkverse: A Multi-Perspective Analysis of the Negative Societal Impacts of the Metaverse*, 2525 INFO. SYS. FRONTIERS 2071 (June 2, 2023).

[25] Sameer Hinduja, *The Metaverse: Opportunities, Risks, and Harms*, CYBERBULLYING RSCH. CTR., https://cyberbullying.org/metaverse [https://perma.cc/A3VP-Q6PN]; Maria Noemi Paradiso, Luca Rollè & Tommaso Trombetta, *Image-Based Sexual Abuse Associated Factors: A Systematic Review*, 39 J. FAM. VIOL. 931 (Apr. 25, 2023).

[26] Kerr, *supra* note 3; *see also* Balkin, *supra* note 3, at 2045; Hunter & Lastowka, *supra* note 3, at 294.

metaverse are already causing concrete harms "outside the game" and that more of these harms will predictably come as the metaverse expands in line with its corporate creators' goals. Further, we pinpoint a clear subset of today's "virtual worlds" for which a "new" [27] remedial framework is needed. Specifically, where the business model being used to draw users into the metaverse replicates that of social media and interactive gaming platforms, we believe that these dilemmas should be solved using our proposed paradigm. One can think of the parts of the metaverse being built around the free-account-formation/audience-monetization business model pioneered by 2-D social media as creating a metaverse that looks like "social media on steroids." In that realm, as we detail below, strategic choices made by corporate creators have made the "game" of the metaverse so unwieldy that policing harms through a criminal law framework will systematically fall short.

Social media platforms' fundamental corporate strategy for the past decade has been to pursue massive user growth by offering free and frictionless sign-ups, in order to capitalize on network effects and capture natural monopolies. [28] This strategy systematically creates what we coin here to be the "veil of scale," a de facto shield against accountability generated by the trivial ease through which online personae can be created and digital tools can multiply their reach, delivering harmful, deceptive, or manipulative content to dozens, thousands, or tens of thousands of targets with ease.[29] Bad actors are able to

---

[27] Of course, as we detail in Section IV.B., *infra* our "new" model is very old indeed.

[28] *See, e.g.*, PETER THIEL, ZERO TO ONE: NOTES ON STARTUPS AND HOW TO BUILD THE FUTURE (2014). For a discussion of the entwined history of Silicon Valley, social media, and venture capital, see MAX FISHER, THE CHAOS MACHINE: THE INSIDE STORY OF HOW SOCIAL MEDIA REWIRED OUR MINDS AND OUR WORLD (2022).

[29] *See, e.g.*, Joseph Cox, *The $2,000 Phones that Let Anyone Make Robocalls*, 404 MEDIA (Nov. 14, 2023, 9:00 AM), https://www.404media.co/buy-fraud-phone-russiancoms-robocalls/ [https://perma.cc/8CFT-HD63]; Spencer Feingold & Johnny Wood, *'Pig-Butchering' Scams on the Rise as Technology Amplifies Financial Fraud, INTERPOL Warns*, WORLD ECON. F. (Apr. 10, 2024), https://www.weforum.org/stories/2024/04/interpol-financial-fraud-scams-cybercrime/ [https://perma.cc/2W2U-A4JN]. For further discussion of the veil of scale, see *infra*, Section II.D.

hide behind the veil of scale, and criminal or civil actions are systematically unable to reach them through it. Even when existing statutes are, in theory, fully applicable to individual bad actors who commit harms within virtual settings, our current legal and law enforcement infrastructure offers few real options for redress when the actor who commits the harm is anonymous and ephemeral.[30]

This breakneck creation of de facto unpoliceable virtual spaces is neither happenstance nor inevitable. Rather, it is a result of a specific set of business model choices by specific corporations and their investors—choices that have been very successful at privatizing the profits and socializing the costs of pushing vast swathes of formerly real-life human interaction online. Enabled by constantly growing computational power and storage capacity, digital entrepreneurs have entered and disrupted arena after arena of social and economic life, a phenomenon Silicon Valley venture capitalist Marc Andreessen famously described as "software eating the world."[31] The unfolding results continue to outpace efforts of scholars, practitioners, legislators, and policymakers to provide robust accountability structures.

Not all of the metaverse is social media or interactive gaming; not all social media or interactive gaming is the metaverse. But there is a significant and growing area of

---

[30] One tactic that legislators and civil society organizations have pursued is to advocate against anonymity and end-to-end encryption, or demand age-verification, which many experts argue will bring an end to the possibility of anonymity for anyone. *See, e.g.*, Eric Goldman, *Will California Eliminate Anonymous Web Browsing? (Comments on CA AB 2273, The Age-Appropriate Design Code Act)*, TECH. & MKTG. L. BLOG (June 27, 2022), https://blog.ericgoldman.org/archives/2022/06/will-california-eliminate-anonymous-web-browsing-comments-on-ca-ab-2273-the-age-appropriate-design-code-act.htm [https://perma.cc/7E7Q-VB7W]; Jason Kelley & Adam Schwartz, *Age Verification Mandates Would Undermine Anonymity Online*, ELEC. FRONTIER FOUND. (Mar. 10, 2023), https://www.eff.org/deeplinks/2023/03/age-verification-mandates-would-undermine-anonymity-online [https://perma.cc/KUD2-SDWR].

[31] Marc Andreessen, *Why Software Is Eating the World*, WALL ST. J. (Aug. 20, 2011), https://www.wsj.com/articles/SB10001424053111903480904576512250915629460.

overlap. This area of overlap, we will detail, already generates significant substantive problems—and, we argue, will generate predictable jurisprudential dilemmas. Core elements of black letter internet law (Section 230 first and foremost) preceded the dawn of social media, but over the past two decades social media systems and internet jurisprudence have been evolving together. When metaverse platforms make interactions with other users or user-generated content central to the experiences they offer, courts will look to precedents from non-immersive social media cases to guide their rulings.[32]

Thus, an analysis of potential responses to harm in the metaverse requires us to attend to social media precedents, but also to spell out their limits. Immersive virtual reality technology places the ephemeral, the gestural, and the experiential at the center of the online interaction it fosters. Much of the jurisprudence around Section 230 is grounded in discussions of content: who created "the content," and who should choose whether to "leave it up" or "take it down."[33] Addressing such questions, jurists have been able to continue treating social media platforms as analogous to 1990s-era "communication and information retrieval methods":[34] that is,

---

[32] Indeed, lawyers are already prognosticating on ways in which courts will draw from non-immersive cases to create legal rulings related to the metaverse. *See, e.g.*, Tom Ara, Mark Radcliffe, Michael Fluhr, Katherine Imp, *Exploring the Metaverse: What Laws Will Apply?*, DLA PIPER (June 19, 2022), https://www.dlapiper.com/es-pr/insights/publications/intellectual-property-news/2022/exploring-the-metaverse-ipt-news-june-2022 [https://perma.cc/6M3M-5772].

[33] See taxonomy laid out in Eric Goldman, *Content Moderation Remedies*, 28 MICH. TECH. L. REV. 1, 23–40 (2021). For recent empirical analyses of how content moderation works in practice, highlighting the complex interplay of sociotechnical systems that may better be approached as fundamental matters of administration or governance, see Kate Klonick, *The New Governors: The People, Rules, and Processes Governing Online Speech*, 131 HARV. L. REV. 1598 (2018); Evelyn Douek, *Content Moderation as Systems Thinking*, 136 HARV. L. REV. 526 (2022); Tarleton Gillespie, *Platforms Are Not Intermediaries*, 2 GEO. L. TECH. REV. 198 (2018).

[34] These are the words of the Supreme Court used in describing the Communications Decency Act in 1997. Reno v. ACLU, 521 U.S. 844, 851 (1997).

as *conduits of speech*. We argue that with the arrival of the metaverse, that analogy has reached its outer limits. The companies creating the metaverse-as-social-media-on-steroids are building *engineered spaces of interaction*, and jurists should approach them as such.[35]

This dynamic is central to our key argument regarding the compatibility of a premises liability framework within the boundaries of Section 230's existing jurisprudence. We point to swathes of harm that are common in today's non-immersive social media and already documented in the social media and interactive gaming realms of the incipient metaverse. This includes harms where the criminal or tortious interaction remains fully within virtual space, with the tortfeasors acting behind the shield of the "veil of scale." Under such circumstances, which are systematically generated by monetization models of social media and free-to-play gaming, the argument that anyone other than the platform might be able to intervene to prevent or police the harm crumbles.[36] The harms we seek to address are not tortious speech, but rather torts or crimes committed *through* speech, with speech defined broadly to encompass not just verbal but gestural, somatic, and auditory interaction. To recognize a platform's unique sightlines into—and thus, its unique ability to address—harmful acts within spaces that it has engineered and controls, does not require treating it as a publisher or speaker of other people's words under Section 230.[37]

---

[35] Increasing reliance by platforms on generative AI to produce platform content will make the distance from the past model of internet service providers that transmitted individual-user-made content even sharper. *See* Kali Hays, *Big Tech Has Long Avoided Responsibility for Online Content. Generative AI Could End That*, BUS. INSIDER (Dec. 18, 2023, 2:00 AM PST), https://www.businessinsider.com/generative-ai-big-tech-responsible-online-content-section-230-2023-12 [https://perma.cc/A8JU-6RUN].

[36] By, among other things, crashing into the limits of the Fourth Amendment. *See* discussion *infra* Section III.A.

[37] Although outside the scope of this Article, we recognize that there is value in analyzing the effect of diffuse harms from the perspective of collective rights. To our knowledge no one has yet discussed the collective

Thus, with technology hurtling into an unpredictable future,[38] we suggest that the best way to move *forward* in creating a liability framework is to look *back* at the common law of torts and specifically, premises liability for venue owners. Premises liability provides a path to hold corporations liable for the harms their engineered venues create by incentivizing them to use their superior knowledge of ongoing risks within their properties to prevent harm to others—just as premises law has done with regard to physical space for centuries. [39] Crucially, premises liability provides a well-developed model for how to assess (and delimit) responsibility for third-party harm. This model stems from the responsibility assigned to innkeepers from the early English common law and expanded to modern actors such as store owners, who must protect their customers from harms that may occur within their shop. This Article argues that this responsibility can be further expanded and appropriately attributed to the corporate hosts who invite us in to their interactive online realms.[40]

In Part I, we discuss the history of the underlying technology, juxtaposing the vision of many scholars at the dawn of its creation with the way the technology has actually evolved. As data-aggregating social media corporations have sought to pull ever-wider swathes of human interaction onto their platforms, laws such as Section 230 have become increasingly poorer fits. This, combined with the creation and

---

harms of the metaverse, and – as such this would be a fruitful research. To that end, any work on the subject would build from other works. *E.g.*, MARIANNA OLAIZOLA ROSENBLAT, N.Y.U. STERN CTR. FOR BUS. AND HUM. RTS., REALITY CHECK: HOW TO PROTECT HUMAN RIGHTS IN THE 3D IMMERSIVE WEB (2023).

[38] *See, e.g.*, SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT THE NEW FRONTIER OF POWER (2019) (discussing these harms as analogous to the diffuse harms present in environmental pollution).

[39] Robert S. Driscoll, *The Law of Premises Liability in America: Its Past, Present, and Some Considerations for Its Future*, 82 NOTRE DAME L. REV. 881 (2006).

[40] Whether the same reasoning we present in this Article could be used to justify the extension of the premises liability paradigm to harms in non-immersive online spaces—that is, social media outside the metaverse—is not a question we address here.

commercialization of the technology necessary for immersive interactions, is the evolution, we argue, that cements the era of platforms-as-premises.[41]

In Part II, we discuss a range of harms that are occurring or are expected to occur in the metaverse, including harms relating to ownership rights, harms relating to false simulations that promise something different than what is actually delivered, and physical and emotional harms to persons. We argue that the legal system's ability to respond appropriately to prevent or punish these harms will vary systematically, depending on the business model and monetization scheme of the platform within which the harm occurs. Those parts of the metaverse built around frictionless account-formation, such as social media's audience-monetizing scheme or online gaming's micro-payment-driven scheme, will predictably be beset by de facto unpoliceable third-party harms, just as their non-immersive online counterparts already are. These third-party harms will not only include exposure to violent or disturbing content, but also manipulation or extortion that will lead to violations of self and trust, image-based sexual abuse, child sexual exploitation, and invasion of privacy. Meanwhile, as ever larger portions of the world's population come online, and off-the-shelf digital tools speed access to translation and digital facsimiles, the possibilities for bad actors to find targets and victimize them will predictably grow.

In Part III, we return to the real world. Specifically, we analyze the shortcomings of existing legal remedies and assess some of the current statutes that intersect with the metaverse. We conclude that while approaches like data-privacy and antitrust could be part of an accountability framework in the future, achieving success through those models will require challenging the fundamental business model and governance structure of internet access. These are not quick fixes. Meanwhile, multiple existing statutes regarding economic and personal harms are, in theory, already fully applicable to real-world harms committed via virtual interaction. In practice, however, our law enforcement and judicial infrastructure

---

[41] See discussion *infra* Sections I.A & I.D.

offers little redress when the person who commits that harm does so via an account or avatar that is anonymous and ephemeral, which is a circumstance that platforms not only permit but *rely on* for user growth. Tortfeasors are hidden from accountability by the "veil of scale."[42]

Enter premises liability.

In Part IV, we discuss the common law of torts, in general, and premises liability, specifically, to advocate for their use in the metaverse. We detail the specific elements of the premises liability tradition that make it an optimal model for holding platforms responsible for harms committed by third parties within the risk-laden virtual settings that platforms own, run, and profit from. The premises framework provides a path of redress for victims of foreseeable, preventable, and egregious harm, while also recognizing that not all harms are preventable and not all precautions are reasonable. It is in Part IV that we make the argument at the heart of this Article—that as we face emerging harms facilitated by a new, engineered space of interaction, premises liability offers a familiar legal paradigm that (1) has sound jurisprudential foundations, (2) is well-aligned (for concrete technological reasons) with dilemmas of place-built risk and third-party harms, and therefore (3) can be taken with minimal adjustments and applied to harms effectuated in the metaverse.[43]

In the end, we are not so naïve as to think that applying this

---

[42] On the role of the Fourth Amendment in limiting law enforcement access to data that captures harm-doing at scale, see discussion *infra* Section III.A.

[43] Note that courts have already grappled with how to analogize physical property to virtual property in the development and affirmation of the concept of cybertrespass. *See* Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468 (Cal. Ct. App. 1996); CompuServe v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997). Indeed, some analysts have raised the question of whether the common law of realty would be a more appropriate model for digital property than that of chattel. *See, e.g.*, Shyamkrishna Balganesh, *Common Law Property Metaphors on the Internet: The Real Problem with the Doctrine of Cybertrespass*, 12 MICH. TELECOMM. & TECH. L. REV. 265 (2006); Adam MacLeod, *Cyber Trespass and Property Concepts*, 10 IP THEORY Art. 4 (2021), https://www.repository.law.indiana.edu/ipt/vol10/iss1/4 [https://perma.cc/UJD5-MZ26] (discussing the law with regard to license to enter).

framework will solve all of the issues that will invariably arise in this space. Nor are we dismissive of the argument that technology is changing too fast for the law to catch up. In fact, it is *because* of this sense of rapidity that we argue that what is needed, at this moment, is a tried-and-true framework for assessing the obligations of owners for risks and harms on properties they control.

Sometimes (just sometimes), the old ways really are the best.

I. This Section is Already Out of Date – the Breakneck Speed of Technological Changes

> *When Hiro goes into the Metaverse and looks down the Street and sees buildings and electric signs stretching off into the darkness, disappearing over the curve of the globe, he is actually staring at the graphic representations – the user interfaces – of a myriad different pieces of software that have been engineered by major corporations.*[44]

In the time that it will take you to read this Section, some new technological innovation may already have appeared on the market. From our social connections to our shopping habits, from the way that we communicate to the ways we isolate, digital technology has been at the heart of some of the most rapid changes society has ever seen—even before the immersive digital interface Stephenson predicted for Hiro in *Snow Crash*. One obvious example is generative AI which, since the recent debut of its exemplar (Chat GPT) in November 2022, has already caused technological, industry and even societal disruption. [45] Similarly, recent advances in

---

[44] STEPHENSON, *supra* note 1, at 31.

[45] In the three years since ChatGPT has debuted, there have been an ever-increasing call among academics to heed the incredible upending that the technology could have for the profession. *See, e.g.*, Andrew M. Perlman,

computational power, machine learning, and graphics processing have brought experiences approaching Stephenson's metaverse nearer to the realm of possibility.

At its most basic, virtual reality involves a move from viewing things on a flat screen to becoming a part of the screen and surrounding environments, via a technological interface that uses wearable devices (e.g., headsets, goggles, microphones, earpieces, and gloves) as input and output devices. [46] These devices, via high-speed wireless data transmission to a shared platform, enable real-time interaction with digital settings and the images or "avatars" of other users, generating an illusion of immersive reality.[47]

But "the metaverse" requires more than just sophisticated devices for viewing things. It depends upon an infrastructure for development and interoperability such that when you turn those devices on, there will be something to do: some game to play, some training to complete, something to buy, someone to meet.[48] These digital activities are not being built in a vacuum.

Generative AI and the Future of Legal Scholarship (Mar. 3, 2025) (unpublished manuscript) (available on SSRN), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5072765 (taking the unique approach of having ChatGPT **write** most of the article discussing where it should fit within legal scholarship). For a more comprehensive discussion of the disruptive impact of AI, *see* Jena Martin & Ritu Narula, *Balancing Interests: AI, Business and Human Rights and the Legal Landscape in an Era of Disruption*, 127 W.VA. L. REV. 1 (2024).

[46] T.C., *How Virtual Reality Works*, ECONOMIST (Sept. 1, 2015), https://www.economist.com/the-economist-explains/2015/09/01/how-virtual-reality-works [https://perma.cc/DKH8-E4KT].

[47] In his book VIRTUAL REALITY, Steven M. LaValle provides a more esoteric definition that aligns with our discussion above. LaValle's definition of virtual reality is "inducing targeted behavior in an organism by using artificial sensory stimulation, while the organism has little or no awareness of the interference." STEVEN M. LAVALLE, VIRTUAL REALITY 1 (2023). According to LaValle, there are four components to virtual reality: (1) creating targeted behavior; (2) on an "organism" (usually, but not always, a human); (3) using "artificial sensory stimulation;" (4) that leads the organism to being "fooled" into immersion in a virtual world. *Id.* at 1-2.

[48] For an overview of the many technical components needed to build the metaverse infrastructure see *What components are part of Metaverse*

Rather, the crucial corporate players, financing structures, technological protocols, legal landscape, and approaches to monetization in the metaverse are those that have developed over the past three decades of tech-sector growth, with the rise of social media platforms playing a starring role in that story.[49]

The late 1990s and early 2000s saw a surge of interest from legal scholars in the governance of "cyberspace."[50] That scholarly literature still has important insights to offer. Yet as is natural, that literature envisioned solutions for "cyberspace" conditioned on the socio-technical and business models of its era—an era before the rise of social media platforms. This Part will begin by laying out some crucial components of those early arguments on the governance of cyberspace, underlining the

---

infrastructure?, IEEE METAVERSE, https://metaversereality.ieee.org/publications/articles/what-components-are-part-of-mateverse-infrastructure#:~:text=Harnessing%20spatial%20computing%2C%20metaverse%20infrastructure,them%20into%20the%20virtual%20world [https://perma.cc/7M9S-4VPA]. For a discussion of the implications of building this world on businesses see Chris Arkenberg & Jana Arbanas, *What Does it Take to Run a Metaverse?*, DELOITTE (Feb. 20, 2023), https://www2.deloitte.com/us/en/insights/industry/technology/metaverse-infrastructure.html [https://perma.cc/XD7U-XBFP].

[49] *See e.g.*, Marcus Law, *Top 10: Metaverse Companies*, TECH. MAGAZINE (Aug. 7, 2024), https://technologymagazine.com/top10/top-10-metaverse-companies-2024 [https://perma.cc/GHC9-YZU3]; Josephine Walbank, *Top 10 Companies Investing in the Metaverse in 2023*, MOBILE MAGAZINE (Jan. 20, 2023), https://mobile-magazine.com/articles/top-10-companies-investing-in-the-metaverse-in-2023 [https://perma.cc/Z8CH-7F3Z].

[50] *See, e.g.*, Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1679 (1995); David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996); Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119 (1998); Amy Lynne Bomse, *The Dependence of Cyberspace*, 50 DUKE L.J. 1717 (2001); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons,* 91 CALIF. L. REV. 439 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV 521 (2003); Lastowka, F. Gregory & Dan Hunter, *The Laws of the Virtual Worlds*, 92 CALIF. L. REV. 1 (2004); H. Brian Holland, *The Failure of the Rule of Law in Cyberspace?: Reorienting the Normative Debate on Borders and Territorial Sovereignty*, 24 J. MARSHALL J. COMPUTER & INFO. L. 1 (2005).

ways their envisioned pathways presumed that virtual space would continue to consist of community-driven, sustained human collectives. We then track the actual pathways of cyberspace, focusing on the development of engagement-maximizing social media and its accompanying profit models. The end result, we argue, is that most of today's online worlds are spaces of ephemeral and easily deceptive interaction that upend the foundational presumptions of early debates over cyberspace self-governance. Accelerated by social media engagement algorithms and AI-powered tools, internet anonymity is no longer a matter of a single soul typing away, happy that (in the words of the 1993 *New Yorker* cartoon) "[o]n the Internet nobody knows you're a dog."[51] Today, guides on how to run a slew of simultaneous deceptive accounts across multiple languages to execute romance scams or "sextortion" are openly available on TikTok and YouTube as well as "dark web" forums;[52] tens or hundreds of thousands of fake followers are routinely bought and sold; [53] ad fraud "click farms" proliferate;[54] automated deep fake "AI Instagram influencers" capitalize on real sex workers' (stolen) likenesses.[55] We detail the entwined evolution of technology, venture capital, and monetization strategy that undergird these social media

---

[51] On the Internet, *Nobody Knows You're a Dog*, WIKIPEDIA, https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog (last visted Mar. 21, 2025).

[52] Lora Kolodny, *Sextortion Training Matrials Found on Tiktok, Instagram, Snapchat and Youtube, According to New Report*, NBC NEWS (Jan. 27, 2024, 6:00 AM), https://www.nbcnews.com/tech/internet/sextortion-yahoo-boys-snapchat-tiktok-teen-wizz-rcna134200.

[53] Dan Whateley, *The FTC is Coming After Influencers and Brands that Buy Fake Followers*, BUS. INSIDER. (Aug. 10, 2024, 8:35 AM), https://www.businessinsider.com/influencers-and-brands-ftc-says-you-cant-buy-fake-followers-2024-8.

[54] Jason Koebler, *Facebook's Algorithm Is Boosting AI Spam That Links to AI-Generated, Ad-Laden Click Farms*, 404 MEDIA (Mar. 19, 2024, 9:19 AM), https://www.404media.co/facebooks-algorithm-is-boosting-ai-spam-that-links-to-ai-generated-ad-laden-click-farms/.

[55] Jason Koebler, *'AI Instagram Influencers' Are Deepfaking Their Faces Onto Real Women's Bodies*, 404 MEDIA (Apr. 9, 2024, 10:47 AM), https://www.404media.co/ai-influencers-are-deepfaking-their-faces-onto-real-womens-bodies/.

realities. We then show that key elements of the social media engagement economy are replicated in the emerging metaverse. Finally, we sketch out the range of use cases that investors are promising to pursue.

A. The Socio-Technical Predicates of 1990s Internet Self-Governance Debates

It is not happenstance that Stephenson's envisioned "metaverse" dates to 1992. The early 1990s saw the first spread to the general public of personal computers linked via dial-up connection to the internet,[56] the first embrace of online fora for real-time social interaction, and the first widespread discussion of harms and disputes within them. One incident would become a touchpoint for much subsequent theorizing, in part because a journalist happened to be present. [57] In LambdaMOO, [58] an entirely text based ongoing multi-user domain with 1,500 active users at the time,[59] a player known as Mr. Bungle virtually attacked others, using a subprogram that

---

[56] PAUL E. CERUZZI, COMPUTING: A CONCISE HISTORY (2012).

[57] Julian Dibbell, *A Rape in Cyberspace or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database into a Society*, 1994 ANN. SURV. AM. L. 471 (1994). Among many subsequent engagements by scholars, see Richard MacKinnon, *Virtual Rape*, 2 J. OF COMP.-MEDIATED COMM., no. 4 (1997); Laurie Johnson, *Rape and the Memex, in* REFRACTORY, J. OF ENTERTAINMENT MEDIA (2008); John Danaher, *The Law and Ethics of Virtual Sexual Assault, in* BARFLIED, W. AND BLITZ, M. RESEARCH HANDBOOK ON THE LAW OF VIRTUAL AND AUGMENTED REALITY 363-89 (Cheltenham, Edward Elgar Publishers, 2018).

[58] A "MOO" stands for a Multi-user, Object Oriented space and represents the earliest seeds for today's metaverse. The key difference between a MOO and today's immersive reality is the MOOs' text-based interaction, without other visual or tactile elements. *See* Peter Ludlow, *The Government of LambdaMoo,* STANFORD (2001), https://cs.stanford.edu/people/eroberts/cs181/projects/online-governance/governance-structures/lambda-moo.html [https://perma.cc/2AE2-2YVM].

[59] Charles J. Stivale, *Spam: Heteroglossia and Harassment in Cyberspace, in* INTERNET CULTURE 94-95 (David Porter ed., Routledge 1997); *see also* Charles J. Stivale, *"help manners": Cyber-Democracy and its Vicissitudes,* 1 ENCULTURATION, No. 1 (Spring 1997), https://enculturation.net/1_1/stivale.html [https://perma.cc/H5E3-R4HR].

attributed sentences to them which described them committing explicit acts of sexual violation. In response, the participants who had been victimized and other community members convened a public virtual forum, where there was extensive debate about appropriate consequences for Mr. Bungle. Ultimately one of the domain's administrators ("wizards") permanently erased (or "toaded") the Mr. Bungle character, a step that some community members supported while others worried had not followed proper process. In the wake of these traumatic events, the programmers who had created LambdaMOO no longer wished to be solely responsible for policing behavior there. As a result, they developed formal procedures for presenting and voting on propositions and adjudicating consequences.[60]

Julian Dibbell, the LambdaMOO participant who chronicled these events shortly afterward in a piece titled "A Rape in Cyberspace,"[61] saw in the improvised and fractious but ultimately effective response an illustration of the nascent processes through which structures for self-governance in online spaces could arise. As he writes,

> Since getting the wizards to toad Mr. Bungle (or to toad the likes of him in the future) required a convincing case that the cry for his head came from the community at large, then the community itself would have to be defined; and if the community was to be convincingly defined, then some form of social organization, no matter how rudimentary, would have to be settled on. And thus, as if against its will, the question of what to do about Mr. Bungle began to shape itself into a sort of referendum on the political

[60] Dibbell, *supra*, note 57, at 477-85. For a more detailed description of the creation and subsequently evolution of governance and quasi-legal procedures, see Jennifer L. Mnookin, *Virtual(ly) Law: The Emergence of Law in LambdaMoo*, 2 J. OF COMP.-MEDIATED COMM., no. 1 (1996).

[61] First published December 21, 1993; Reprinted in the *Village Voice* in 2018 at https://www.villagevoice.com/a-rape-in-cyberspace/.

future of the MOO.[62]

Even though, as Dibbell tells us, the person who had created the Mr. Bungle persona circumvented the banishment by creating a new internet account and re-registering, they had been chastened by the experience and were now "a lot less dangerous to be around."[63] And more broadly, LambdaMOO's nascent structures of participatory governance seemed to have succeeded in enabling the elaboration and enforcement of pro-social rules and the sanctioning of harmful behaviors. "Eight months and 11 ballot measures later, widespread participation in the new regime has produced a small arsenal of mechanisms for dealing with the types of violence that called the system into being."[64]

The points of difference between the LambaMOO "cyberspace" of 1993 and the "metaverse" of 2025, whose present and predictable harms the present Article explores, are profound, and they shed critical light on the implicit assumptions within early legal theorizations of how law should work in then-emergent internet realms.[65]

---

[62] Dibbell, *supra*, note 57 at 479.

[63] *Id.* at 487.

[64] *Id.* at 485.

[65] Separately from the issues discussed above, one of the clearest differences from the hobbyist work of 1993 is today's massive presence of children in online spaces with no parental supervision: a presence actively encouraged by companies such as Roblox, as we detail below. In Part II of this Article, we will talk about predictable harms in the metaverse, underlining among other things that when children are involved—and especially when those children have access to internet-linked devices with cameras—virtual sexual aggression is not just about using words that make fellow game-players uncomfortable. Rather, it is definitionally non-consensual sexual exploitation and often solicitation of CSAM (child sexual abuse material, formerly termed child pornography) and hence constitutes multiple different crimes. *See e.g.* discussions in *Teaching Module Series: Cybercrime, Online Child Sexual Exploitation and Abuse*, UNITED NATIONS OFF. ON DRUGS AND CRIME, https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-12/key-issues/online-child-sexual-exploitation-and-abuse.html; U. S. Gov't Accountability Off., GAO-23-105260, ONLINE EXPLOITATION OF

Journalists, participants, and law professors writing in the 1990s assumed "the internet" was inherently a realm of decentralized, human-scaled, voluntary interaction, with technical parameters well understood by savvy and intentional participants who are able to opt in or opt out at will; a landscape offering more freedom and autonomy than the physical world, rather than more opacity and surveillance; and a space within which individuals and governments dispute the boundaries of privacy, but profit-driven corporations play no meaningful role.[66] That is not the internet of today.

As we will detail below, today's internet is routinely accessed via social media platforms designed to attract participants at a massive scale. Such spaces are engineered for frictionless entry and group formation, reliant on the ease of creation of ephemeral accounts. To join a new platform, you create an account by providing a few non-verified personal details and clicking through terms of service. While social media platforms track your account's interactions in fulsome automated detail, and both they and other online sites and advertisers track your movements between online spaces via recognition of your device/s and sometimes your IP address, none of this is transparently identifiable by other users online.[67]

CHILDREN: DEPARTMENT OF JUSTICE LEADERSHIP AND UPDATED NATIONAL STRATEGY NEEDED TO ADDRESS CHALLENGES (Dec 14, 2022), https://www.gao.gov/assets/d23105260.pdf [https://perma.cc/6TXD-65D4].

[66] These shared assumptions underly the otherwise quite distinct views of internet regulation in, e.g., David G. Post, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace*, 1995 J. ONLINE L. art. 3; Timothy S. Wu, *Cyberspace Sovereignty?—The Internet and The International System*, 10 HARV. J. OF L. & TECH. 647 (1997); John Perry Barlow, *A Declaration of the Independence of Cyberspace*, 18 DUKE L. & TECH. REV. 5, 5 (2012) (originally published on Feb. 8, 1996). The initial investment undergirding the development of internet protocols and connections was subsidized by the U.S. federal government, first in the form of ARPANET and then under the aegis of the National Science Foundation, together with academic institutions. By the 1990s, individual users were paying broadband internet service providers for modems and routes to connect into this system. *See* Roy Rosenzweig, *Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet*, 103 AM. HIST. REV. 1530 (1998).

[67] *See* discussion in Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization,* 30 J. OF INFO. TECH. 75 (2015).

One person can run thousands of accounts claiming different identities, or shed them at will.[68] Groups, in turn, may be small or massive, hidden or public, and as ephemeral as the accounts participating in them. Such spaces are routinely characterized not by the slow building of norms but rather by the loud presence of participants with no interest in collaborative rule-making or the sustainable structures for deliberative problem-solving.[69] Meanwhile, even if they were able to deliberate and reach collective agreements, participants in today's social media platforms—with their millions or even billions of daily users—have no possibility of two-way communication with the individuals writing the code or making decisions about how to apply rules.

In LambdaMOO, in contrast, participants were pseudonymous but neither anonymous nor ephemeral. A critical mass of people had built relationships over time with each other, and this undergirded the deliberative dialogue through which people came to agree that an offense had been committed and punishment was merited. Community participants also had a direct line of public communication to those running the code, creating both leverage and trust. Not only was one of the "wizards" persuaded, by his participation in the heartfelt communal discussion, to banish the harm-doer, but also the "wizards" further responded to the need for collaborative governance by creating, maintaining, and deferring to formal voting and conflict arbitration systems. Finally, although there was at least one intentional harm-doer in LambdaMOO, doing harm was seemingly not prevalent within that interactive space. On the contrary, the harm committed was a violation of local norms. As such, the creation of the formalized structures to reinforce those norms and prevent such harms did not run counter to the site's fundamental value-proposition for either its users or its

---

[68] Koebler, *supra* note 54; Jason Koebler, *Where Facebook's AI Slop Comes From*, 404 MEDIA (Aug. 6, 2024, 10:05 AM), https://www.404media.co/where-facebooks-ai-slop-comes-from/.

[69] On the failures of cooperative deliberation and prevalence of tribalized outrage on social media platforms, see FISHER, *supra* note 28 AT 13-66.

creators.[70]

Thus, we recognize four primary factors that differentiate LambdaMOO from the social media/online gaming realms of today's metaverse: (1) the small scale of the community, with participants numbering only in the thousands; (2) the lack of monetization related to interactions within that community; (3) the lack of investor-led pressure to maximize the user base in order to drive profits, and; (4) the non-ephemeral (even when pseudonymous) identities of the people who were interacting within that community. These socio-technical and infrastructural predicates are important not only in regard to the specific issue of preventing or punishing sexual harms in virtual spaces, but also with regard to our broader case for the

---

[70] For position statements from practitioners directly connected to the "Mr. Bungle" events, see Amy Bruckmen, Pavel Curtis & Cliff Figallo, *Approaches to Managing Deviant Behavior in Virtual Communities*, DIAC WORKSHOP 183-84 (Apr. 24-28, 1994). Pavel Curtis was a Xerox researcher and LambdaMOO's principal architect, and in his role as "archwizard" it was he who instituted the formal system for ballot measures and voting on violations in the aftermath of Mr. Bungle's attacks and banishing. Dibbell, *supra*, note 57 at 485. Amy Bruckman was then a doctoral candidate at MIT and creator of the virtual reality community MediaMOO. She wrote,

> social solutions require time, effort, and leadership. Being able to take the time to engage each problem user in a dialogue is a luxury that comes from having a small community size. Larger communities necessarily become bureaucracies; in a real sense, they cease to be communities at all. I will propose a model of clusters of small, affiliated communities and sub-communities as a structure for preventing and managing social problems.

Bruckmen, Curtis & Figallo, *supra*, at 184. Figallo, who had been Managing Director of the Whole Earth 'Lectronic Link (WELL), a pioneering online community launched in 1985, in its earliest years, wrote that

> [b]y encouraging the formation of core groups of users who shared their desire for minimal social disruption, management not only relieved itself of the need to intervene as the authority in minor cases of disruption, but it also gained the socializing influence of a dispersed citizenry actively supporting community standards of behavior and passing them on to new arrivals.

Id. For more information on the WELL, see Fred Turner, *Where the Counterculture Met the New Economy: The WELL and the Origins of Virtual Community*, 46 TECH. & CULTURE 485 (2005).

inadequacy of current jurisprudential frameworks for the emerging social metaverse.

Across the 1990s, a vibrant body of literature emerged in which legal scholars debated whether cyberspace was part of the real world, and should be governed by real world regulations, or instead lay beyond the grasp of sovereign nations, and would as a new society develop its own regulatory structures, rules, and systems of rights.[71] Revisiting those early debates today, one is most struck by the actors who were not yet salient: near-monopolistic, highly capitalized, globally impactful social media platforms. It is the route towards growth that those social media platforms have chosen to pursue, and the business model entwined with it, that have created the crucial points of divergence from early 1990s "cyberspace" as epitomized by the LambdaMOO.[72] Today's "cybernauts" are not a select set of hobbyists but rather over sixty percent of the world's population, relying on digital routes for quotidian information, interaction, and hustles.[73]

For the great majority of its five and a half billion users,

---

[71] *See, e.g.*, Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L. J. 1639, 1639-79 (1995); David R. Johnson & David Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996); Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403 (1996); Jack Goldsmith, *Regulation of the Internet: Three Persistent Fallacies*, 73 CHI.-KENT L. REV. 1119 (1998). For broader coverage of historic cyberspace utopianism among practitioners in the early 1990s, see PATRICE FLICHY, THE INTERNET IMAGINAIRE (2008), and the very non-utopian Neal Kumar Katyal, *Criminal Law in Cyberspace*, 149 U. PENN. L. REV. 103 (2001).

[72] *See* Mnookin, *supra* note 60. In passing, and seemingly viewed self-evident, she notes that "it is in those occasions in which the separation ceases to exist, resulting in real damages to a real person, in which the legal system ought to recognize goings-on within Lambda MOO as raising legally cognizable claims" *Id.* at 41. In short, the feasibility of action vis-à-vis those claims was not treated as a fundamental stumbling block. However, it is our contention in this Article that the "veil of scale" created by modern social media's expansion strategy has made it one.

[73] *Individuals Using the Internet*, WORLD BANK GROUP (2023), https://data.worldbank.org/indicator/IT.NET.USER.ZS [https://perma.cc/7DT3-X4UZ].

today's internet is accessed alongside social media.[74] By offering frictionless account formation and sometimes direct subsidies for data access,[75] social media platforms have unlocked vertiginous growth, reaching a scale at which no set of everyday users can feasibly get responsiveness from those

---

[74] There are currently 5.5 billion internet users and 5.25 billion social media users. *Global Internet use continues to rise but disparities remain,* United Nations Dep't of Econ. and Soc. Affairs, https://social.desa.un.org/sdn/global-internet-use-continues-to-rise-but-disparities-remain [https://perma.cc/LG5L-7AP8]; *Global Social Media Statistics*, Data Reportal, https://datareportal.com/social-media-users [https://perma.cc/5AXR-BSNV].

[75] Subsidies function via zero-rating,

> a practice where companies and internet service providers (ISPs) offer mobile phone users free access to parts of the internet i.e., the ability to visit certain sites and use certain applications without it counting towards your data usage. For instance, Facebook may agree with an ISP that all the ISP's customers can enjoy unlimited use of Facebook without it contributing to their data usage. In this scenario, while anything else you do with your data will count towards your total data usage, you can use Facebook as much as you like.

Aishwarya Shaji, *Is Zero-Rating a Threat To Human Rights?*, HUM. RTS. PULSE (Jan. 22, 2022), https://www.humanrightspulse.com/mastercontentblog/is-zero-rating-a-threat-to-human-rights#:~:text=Zero%2Drating%20refers%20to%20a,as%20much%20as%20you%20like [https://perma.cc/Z7KD-VMQG]. Poverty drives dependence on such subsidies. As the UN notes, "The cost of a fixed-broadband subscription in low-income countries is the equivalent of nearly a third of the average monthly income." United Nations Dep't of Econ. and Soc. Affairs, *supra* note 74. On the reach of Facebook Zero *see* Christopher Mims, *Facebook's Plan to Find Its Next Billion Users: Convince Them the Internet and Facebook Are the Same*, QUARTZ (Sept. 24, 2012) https://qz.com/5180/facebooks-plan-to-find-its-next-billion-users-convince-them-the-internet-and-facebook-are-the-same [https://perma.cc/H6KU-7K7S]. In 2014, between one-half and two-thirds of survey respondents in Brazil, India, Indonesia, and Nigeria agreed with the statement "Facebook is the Internet." Leo Mirani, *Millions Of Facebook Users Have No Idea They're Using The Internet*, QUARTZ (Feb. 9, 2015) https://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet [https://perma.cc/74PG-MHB2].

running the system.[76] Within this structure, users are not the customers but rather the product being sold, their attention monetized via algorithmic ad auctions. Network effects create natural monopolies that limit users' ease of exit. And users' negative experiences routinely fail to gain the ear of those with the power to change the platforms, taking a back seat to a profit mandate that seems to require prioritizing growth over all else.[77]

Because the socio-technical and financial developments that shaped social media platforms across the last 20 years have undercut many of the foundational assumptions of an earlier generation of scholarship on accountability and governance within cyberspace, [78] it will be necessary for us to review the key

---

[76] Despite egregious violations, negative news coverage is routinely required before platforms take action. *See, e.g.*, Jason Koebler, *YouTube Deletes 1,000 Videos of Celebrity AI Scam Ads*, 404 MEDIA (Jan. 25, 2024), https://www.404media.co/youtube-deletes-1-000-videos-of-celebrity-ai-scam-ads/ [https://perma.cc/QWF9-BGMT]; Lara Putnam, *Facebook Has a Child Predation Problem*, WIRED (Mar. 13, 2022) https://www.wired.com/story/facebook-has-a-child-predation-problem/; Lara Putnam, *Latin America's Children at Risk on Facebook: Predators Stalk Children in Celebrity Fan Groups*, TECH POLICY PRESS (Feb. 26, 2025), https://www.techpolicy.press/latin-americas-children-at-risk-on-facebook-predators-stalk-children-in-celebrity-fan-groups/ [*hereinafter* Putnam, *Children at Risk*]; Kashmir Hill, *A Vast Web of Vengeance*, N.Y. TIMES (Jan. 30, 2021), https://www.nytimes.com/2021/01/30/technology/change-my-google-results.html; *see also* Adam Satariano, *'Right to Be Forgotten' Privacy Rule Is Limited by Europe's Top Court*, N.Y. TIMES (Sept. 24, 2019) (discussing disputes over the implementation of the European Union-mandated "right to be forgotten"), https://www.nytimes.com/2019/09/24/technology/europe-google-right-to-be-forgotten.html. For further discussion of the European Union framework, see Samuel W. Royston, *The Right to Be Forgotten: Comparing U.S. and European Approaches*, 48 ST. MARY'S L.J. 253 (2016).

[77] Cory Doctorow has been describing this as the enshittification of the internet. *See, e.g.*, Cory Doctorow, *The 'Enshittification' of TikTok, Or How, Exactly, Platforms Die,* WIRED (Jan. 23, 2023), https://www.wired.com/story/tiktok-platforms-cory-doctorow/.

[78] A fulsome recounting of the evolution of cyberspace governance debates over these subsequent decades is beyond this scope of this Article, but among interventions, see Amy Lynne Bomse, *The Dependence of*

elements of that financial and socio-technical evolution in order to understand the dilemmas now before us.

B. From Dial-up Discussion Boards to Growth-Hacking for Venture Capitalists: The Internet, 1990s-2020s

In this Section we trace the evolution of modern social media platforms and the legal frameworks that have evolved along with them. This is essential for understanding what is to come in the metaverse for three reasons: 1) the same corporations that have been the most successful at parlaying social media or interactive online gaming into exponential growth are the ones now seeking to bring the metaverse into every home; 2) beyond these specific corporate actors, social media's core business model, in which easy, free account creation drives company metrics and stock valuations, is being copied by those who seek to replicate its exponential growth and commensurate profits in the metaverse; and 3) internet law as it has evolved to shield social media platforms from liability for user-generated harm will be treated as precedential for the metaverse. Combined, these three factors generate a significant shortfall of accountability in a particularly insidious way. Specifically, because the result of social media platforms' business model has been the proliferation of ephemeral and

---

Cyberspace, 50 DUKE L. J. 1717 (2001); Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons,* 91 CALIF. L. REV. 439 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV 521 (2003); Lastowka, F. Gregory, and Dan Hunter, *The Laws of the Virtual Worlds*, 92 CALIF. L. REV. 1 (2004); H. Brian Holland, *The Failure of the Rule of Law in Cyberspace?: Reorienting the Normative Debate on Borders and Territorial Sovereignty*, 24 J. MARSHALL J. COMPUTER & INFO. L. 1 (2005); Julie E. Cohen, *Cyberspace As/And Space*, 107 COLUM. L. REV. 210 (2007); Nicolas Suzor, *The Role of the Rule of Law in Virtual Communities*, 25 BERK. TECH. L.J. 1817 (2010); and Julie E. Cohen, *Internet Utopianism and the Practical Inevitability of Law*, 18 DUKE L. & TECH. REV. 85 (2019). We are grateful to Mike Madison at the University of Pittsburgh's School of Law for encouraging us to engage with this literature. For some of his own crucial contributions, see Michael J. Madison, *Social Software, Groups, and Governance*, 2006 MICH. ST. L. REV. 153 (2006); Michael J. Madison, "Information Abundance and Knowledge Commons," *in* USER GENERATED LAW: RE-CONSTRUCTING INTELLECTUAL PROPERTY LAW IN A KNOWLEDGE SOCIETY 28-54 (Thomas Riis ed., 2016).

anonymous accounts, harms committed behind the "veil of scale" have become so ubiquitous in modern online life that we rarely notice them as an artifact of corporate strategy at all.

In just over a quarter century, internet access has gone from being a niche, recreational, luxury good to a fundamental part of the infrastructure of modern economic, civic, and political life. Within the broad category of consumer-facing digital services, social media platforms have experienced the most explosive growth. The total number of social media users worldwide more than tripled between 2012 and 2021. [79] Roughly two-thirds of the world's adult population now has internet access,[80] and industry sources report that the typical internet user spends nearly seven hours per day online, with about one-third of that spent on social media.[81] The average U.S. teenager currently spends nearly five hours per day on social media.[82]

Moreover, a few companies dominate this market share. For instance, Meta owns four of the largest platforms: Facebook (3 billion active monthly users), Instagram (2 billion), WhatsApp (2 billion), and Messenger (1 billion). Another, YouTube (2.5 billion), is owned by Google, the company that also dominates on-line search and digital advertising. [83] Not coincidentally, Alphabet, the parent company of Google, and Meta are also among the largest

---

[79] Simon Kemp, *Digital 2022: Global Overview Report*, HOOTSUITE 88 (Jan 26. 2022), https://datareportal.com/reports/digital-2022-global-overview-report [https://perma.cc/QLD2-M7TR].

[80] *Id.* at 20.

[81] *Id.* at 18.

[82] Jonathan Rothwell, *Teens Spend Average of 4.8 Hours on Social Media Per Day*, GALLUP (Oct. 13, 2023), https://news.gallup.com/poll/512576/teens-spend-average-hours-social-media-per-day.aspx [https://perma.cc/LUB3-Q8HL].

[83] *Most Popular Social Networks Worldwide as of October 2023, Ranked by Number of Monthly Active Users*, STATISTA (Oct. 2023), https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users [https://perma.cc/2J88-FMDQ]. Two Chinese-owned social media platforms round out the set of social media platforms that, as of 2023, reported over one billion users per month: WeChat (1.3 billion) and TikTok (1.2 billion). *Id.*

corporations by market capitalization in the world today.[84]

How have a handful of enormously profitable platforms come to dominate humanity's routes into online interaction, rather than the decentralized array of digital access providers and web hosting companies who, at the dawn of the internet age, seemed poised to share that role? The answer lies in how technology, business models, legislation, and jurisprudence have co-evolved over the past 30 years: an evolution that created the entities building the metaverse today.

In the 1990s the web seemed, in the words of business bestseller *The Cluetrain Manifesto*:

> a place where people could talk to each other without constraint. Without filters or censorship or official sanction—and perhaps most significantly, without advertising. . . . The attraction was in speech, however mediated. In people talking, however slowly. And mostly, the attraction lay in the kinds of things they were saying. Never in history had so many had the chance to know what so many others were thinking on such a wide array of subjects.[85]

The Communications Decency Act of 1996[86] was consistent with this picture of the technology and how it would be used. Section 230, in particular, offers key insight into legislators' view of the still-nascent internet as fundamentally a conduit for information—in the Section's brief text, the word "information" appears ten separate times.[87] Early libel lawsuits[88] had sparked concern about whether courts assigning

---

[84] As of November 2024, Alphabet is fourth and Meta is seventh. Lyle Daly, *The Largest Companies by Market Cap in 2024*, THE MOTLEY FOOL (Dec. 2, 2024), https://www.fool.com/research/largest-companies-by-market-cap/ [https://perma.cc/5MJT-822W].

[85] CHRISTOPHER LOCKE, DAVID SEARLS & DAVID WEINBERGER, THE CLUETRAIN MANIFESTO: THE END OF BUSINESS AS USUAL 15 (2000).

[86] 47 U.S.C. §§ 223 et. seq.

[87] Counting "informational," eleven. *See* 47 U.S.C § 230 [Hereinafter Section 230].

[88] Stratton Oakmont v. Prodigy Servs. Co., No. 31063/94, 1995 N.Y. Misc. LEXIS 229 (N.Y. Sup. Ct. May 24, 1995).

intermediary liability to interactive computer services (ICSs) for statements users posted on them would exert a chilling effect on the conveyance of speech. In Section 230, Congress determined that ICSs should not be treated like publishers of information who were liable for content, but like printing press makers or mail carriers: entities whose role is to create the tools through which others produce and promulgate information.[89] ICSs would not be held responsible for user content that might be a target for the communications torts: defamation, invasion of privacy, product disparagement, misrepresentation, and so on.[90]

The explicit goal was to empower companies to innovate new technologies and systems that could improve users' experiences.[91] By immunizing companies against lawsuits over what they took down and what they left up, equally, Section 230 erased what would otherwise have been the "moderator's dilemma," as scholar Eric Goldman has named it.[92] That is, without this preemptive liability shield, companies' best defense against lawsuits by aggrieved parties would be to ensure that company agents viewed no content and acted on no content at all.[93] With Section 230's shield in place, ICSs were free to monitor third-party content as much, or as little, as they chose.

---

[89] Section 230(c)(1), *supra* note 87 (stating "no provider or user of an *interactive computer service* shall be treated as the publisher or speaker of any information provided by another *information content provider*") (emphasis added).

[90] David A. Anderson, *Tortious Speech*, 47 WASH. & LEE L. REV. 71 (1990).

[91] *See, e.g.*, Section 230(b), *supra* note 87 (stating it "is the policy of the United States (1) to promote the continued development of the Internet and other interactive computer services and other interactive media; (2)to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation").

[92] Eric Goldman, *An Overview of the United States' Section 230 Internet Immunity*, in THE OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY 154 (Giancarlo Frosio ed., 2020); Eric Goldman, *Sex Trafficking Exceptions to Section 230*, SANTA CLARA U. LEGAL STUD. RCH. PAPER SERIES 2, No. 2017-13 (Sept. 19, 2017), https://ssrn.com/abstract=3038632.

[93] *See* Eric Goldman, *Why Section 230 Is Better Than the First Amendment*, 95 NOTRE DAME L. REV. REFLECTION 33 (2019).

Even as enthusiastic observers hailed the internet as a leveler of hierarchies and democratizer of information,[94] in those same years, other entrepreneurs worked from a very different insight: that network effects in digital goods systematically favor largeness rather than smallness.[95] Once a critical mass of users has chosen your platform, other users have great incentives to select it as well. Additionally, since the replication of computer code can be almost cost free, there is little to stop you from scaling up exponentially to meet demand.[96] In the low-interest-rate era that followed the 2008-09 Great Recession, this was an alluring proposition for venture capitalists, flush with funds and eager to find long shots that might go from zero users to millions, and create huge returns for early investors.[97]

Enter social media. Online social networks on which individuals could create discoverable profiles first emerged in the mid 1990s with platforms like GeoCities and Classmates.com, and then boomed as Friendster and MySpace surged, next to be displaced by Facebook, YouTube, Twitter and Instagram.[98] The emerging recipe for success combined frictionless account creation; recommendation algorithms,

---

[94] *See, e.g.*, MOISÉS NAÍM, THE END OF POWER: FROM BOARDROOMS TO BATTLEFIELDS AND CHURCHES TO STATES, WHY BEING IN CHARGE ISN'T WHAT IT USED TO BE (2013).

[95] *See, e.g.*, CARL SHAPIRO & HAL VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY (1998); Fiona S. Morton et al., *Committee for the Study of Digital Platforms, Market Structure, and Antitrust Subcommittee Report*, UNIV. CHI. BOOTH SCH. BUS. 12 (May 15, 2019), https://research.chicagobooth.edu/-/media/research/stigler/pdfs/market-structure---report-as-of-15-may-2019.pdf [https://perma.cc/9GQX-J4VX]*; see also* Marco Iansiti, *Assessing the Strength of Network Effects in Social Network Platforms* 10 (Har. Bus. Sch., Working Paper No. 21-086, 2021).

[96] FISHER, *supra* note 28.

[97] Alex Hern, *TechScape: The End of the 'Free Money' Era,* GUARDIAN (Apr. 11, 2023), https://www.theguardian.com/technology/2023/apr/11/techscape-zirp-tech-boom [https://perma.cc/89PP-8A8D].

[98] *See* SINAN ARAL, THE HYPE MACHINE: HOW SOCIAL MEDIA DISRUPTS OUR ELECTIONS, OUR ECONOMY, AND OUR HEALTH—AND HOW WE MUST ADAPT 19 (2021).

which ensured a constant stream of available content; and "like," "re-tweet," or "upvote" mechanisms, which served as public signals of social approbation and activated deeply rooted group dynamics.[99]

A final step shaping the profit model of the digital economy was the advent of the smartphone, offering for the first time a computational device that could accompany users' every step and track users' every online move.[100] The smartphone fused one-to-one communications with ubiquitous and instantly transmittable photo and video capacity, and offered a delivery device for a whole new range of physiologically addictive design features.[101]

With ever greater capacity to fine-tune algorithms and maximize individual users' engagement, social media platforms began functioning less as simple conduits for information and more as engineered spaces of human interaction.[102] And the number of humans worldwide entering those spaces was booming. By 2023, nearly half of the population of India, three-fifths of the populations of Mexico and The Philippines, and two-thirds of the populations of Indonesia, China, and Brazil owned smartphones.[103]

A testament to social media companies' fervent pursuit of ever-larger user-bases was their approach to the ever-scarcer terrain of unconnected populations, where the companies might capture the early-arriver's position as gateway to the internet, cornering the benefit of network effects to come. In

---

[99] *See id.*; SIVA VAIDHYANATHAN, ANTI-SOCIAL MEDIA: HOW FACEBOOK DISCONNECTS US AND UNDERMINES DEMOCRACY (2018).

[100] *See* ARAL, *supra* note 98; *see also Defining A Growth Hacker: Three Common Characteristics*, TECHCRUNCH (Sept. 2, 2012), https://techcrunch.com/2012/09/02/defining-a-growth-hacker-three-common-characteristics/.

[101] FISHER, *supra* note 28.

[102] FISHER, *supra* note 28; VAIDHYANATHAN, *supra* note 99; JEFF HORWITZ, BROKEN CODE: INSIDE FACEBOOK AND THE FIGHT TO EXPOSE ITS HARMFUL SECRETS (2023); ARAL, *supra* note 98; Cyphert & Martin, *supra* note 9.

[103] *Top Countries by Smartphone Users*, NEW ZOO (2023). https://en.wikipedia.org/wiki/List_of_countries_by_smartphone_penetration.

developing markets in Latin America, Asia, and Africa, Facebook offered subsidized monthly data to users, essentially paying people to get online to join their social network.[104]

A common saying emerged in this era: "if you're not paying for it, you become the product."[105] Social media users were exactly that, as platforms gathered personal information about masses of users and sold that data to advertisers, who could then use the platforms to deliver advertising to the most desired targets at the most impactful moment. Platforms relied on maximizing the number of total users and engagement to drive higher valuations.[106] Thus, the business model of social media platforms has come to rest on encouraging massive user growth via free and frictionless sign-ups, in order to corner the naturally monopolistic benefits that adhere to first arrivers.[107]

Non-paying users create value for investors by driving up their platform metrics,[108] but the ease with which users can sign up also creates opportunities for exploitation and deception,

---

[104] Toussaint Nothias, *The Rise and Fall… and Rise Again of Facebook's Free Basics: Civil Society and the Challenge of Resistance to Corporate Connectivity Projects*, MIT GLOB. MEDIA TECHS. & CULTURES LAB (Apr. 21, 2020), http://globalmedia.mit.edu/2020/04/21/the-rise-and-fall-and-rise-again-of-facebooks-free-basics-civil-and-the-challenge-of-resistance-to-corporate-connectivity-projects/. *See also supra* note 76.

[105] *See, e.g.*, Scott Goodson, *If You're Not Paying For It, You Become The Product*, FORBES (Mar. 5, 2012), https://www.forbes.com/sites/marketshare/2012/03/05/if-youre-not-paying-for-it-you-become-the-product/?sh=1803eeb5d6ee [https://perma.cc/JRP7-RY5R].

[106] JOSE VAN DIJCK, THE CULTURE OF CONNECTIVITY: A CRITICAL HISTORY OF SOCIAL MEDIA (2013); TIM WU, THE ATTENTION MERCHANTS: THE EPIC SCRAMBLE TO GET INSIDE OUR HEADS (2016).

[107] Moreover, this model has spread beyond social media into other digital services of various sorts. *See* ERIC BENJAMIN SEUFERT, FREEMIUM ECONOMICS: LEVERAGING ANALYTICS AND USER SEGMENTATION TO DRIVE REVENUE (2014).

[108] *See, e.g.*, ANGELA TRAN KINGYENS & BORIS WERTZ, UNDERSTANDING SOCIAL PLATFORMS (Dec. 7, 2016), http://versionone.vc/wp-content/uploads/2016/12/Understanding-Social-Platforms-Dec2016.pdf; *Guide to Understanding Daily Active Users (DAU)*, WALL ST. PREP (Aug. 30, 2023), https://www.wallstreetprep.com/knowledge/daily-active-users-dau/ [https://perma.cc/4JPW-BCC5].

including spam, scams, and deceptive influence campaigns.[109] When these interfere with users' experiences in ways that work against platforms' goals for user retention, platforms put in place some algorithmic detection or disruption mechanisms such as rate-limiting sign-ups or removing accounts whose pattern of posting reveals them as "inauthentic."[110] Questions around the number of authentic users are so fundamental to valuations that assertions on this point can be fundamental to high-profile disputes. For instance, Elon Musk's accusations that Twitter was undercounting the prevalence of automated accounts ("bots") in order to sustain false stock valuation became a key component in Musk's effort to convince a Delaware Chancery judge to allow him to pull out of his commitment to buy Twitter in 2021.[111]

We have discussed the evolution of business models and monetization strategies in detail because it is fundamental to understanding why the "veil of scale" exists today as a fundamental characteristic of today's global social media. As we underlined at the start of this Article, social media is not coterminous with the metaverse. But just as Facebook sought to push smartphones and free data into hands in Myanmar and

---

[109] *See supra* note 68. On the ease through which non-authentic use can ensue, see for example, Charles Arthur, *How Low-paid Workers at 'Click Farms' Create Appearance of Online Popularity*, THE GUARDIAN (Aug. 2, 2013), https://www.theguardian.com/technology/2013/aug/02/click-farms-appearance-online-popularity.

[110] "Inauthentic" is a term of art within social media company's terms of service for distinguishing between accounts that are instantiations of a single human being or identified corporate actor, and accounts that falsely claim to be such. Importantly, there is still some actor involved in the creation and guidance (algorithmic or otherwise) of an "inauthentic" account. Meanwhile, routinely, individuals interacting via online accounts present themselves in deceptive ways, which can range from the harmless to the intensely harmful—for instance, an adult man may adopt the online persona of a teenage girl in order to persuade a male minor to send him sexually explicit self-photographs. "Authenticity," in other words, is not a simple bright line.

[111] Beatrice Nolan, *Elon Musk's Lawyers Say Twitter is Hiding the Identities of Key Staff Who Calculate Bot Numbers*, BUS. INSIDER (Aug. 11, 2022, 4:14 AM PDT), https://www.businessinsider.com/elon-musk-twitter-bots-employees-lawsuit-2022-8 [https://perma.cc/K3GJ-HW42].

Mexico in order to cement its position as the conduit to the internet,[112] Meta now seeks to become the default entryway into the metaverse via the lure of free and frictionless account creation. As such, user experience in key realms of the metaverse will be shaped by the same "veil of scale" that social media's explosively successful business model systematically generates.

C. The Metaverse Arrives: The Diverse Business Models Through Which Interactive, Immersive Virtual Space Will Be Monetized

Multiple labels have emerged for the technologies being built to shape user experiences to create the illusion of the metaverse: artificial reality, virtual reality, immersive reality, and, more recently, extended reality or cross reality.[113] In this Article, we will use the term immersive reality (or IR) for completely immersive creation, like that depicted here:

> Fully-immersive simulations give users the most realistic simulation experience, complete with sight and sound. To experience and interact with fully-immersive virtual reality, the user needs the proper VR glasses or a head mount display (HMD). VR headsets provide high-resolution content with a wide field of view. The display typically splits between the user's eyes, creating a stereoscopic 3D effect, and combines with input tracking to establish an immersive,

---

[112] *See* Shaji *supra* note 75; Nothias *supra* note104.

[113] Many of the distinctions in the varying terms relate to the level of interaction in the "virtual" versus the analog world. For instance, virtual reality (VR) uses different sensory equipment to completely immerse the user in an artificially created environment, reminiscent of the movie, *Ready Player One*. In contrast, augmented reality (AR) allows the user to interact both with the technology and the real-world environment simultaneously (for example, using technology to "place" a holographic piece of furniture in your room.) For a succinct discussion of each (along with an emerging term, "Cross-Reality"), see Stylianos Mystakidis, *Metaverse*, 2022 ENCYCLOPEDIA 486-97 (Feb. 10, 2022).

believable experience.[114]

A hallmark of the IR environment is its immediate response to the end user's input.[115] Evolving devices allow users to engage orally, visually, haptically, and auditorily in a three-dimensional interaction with their surroundings. [116] The immersive nature of the experience, and the ever-increasing ability to make real-time visual renderings more and more realistic, result in intense sensorial impact, including "phantom touch," a tingling sensation that can be generated by perceived contact in IR even absent any physical stimulation.[117]

Wearable IR devices do not themselves constitute a "metaverse." On the contrary they can be (and routinely are) used for individual and private experiences, like virtual bowling in your basement via Nintendo Wii. What makes today's deployment of IR technology different is that it is integrating existing social media, interactive gaming, and digital commerce platforms. Doing so not only requires user-end devices to render immersive experience but also web-based interfaces to which those users can connect, which will

---

[114] *The 3 Types of Virtual Reality*, HEIZENRADER (Sep. 11, 2019), https://heizenrader.com/the-3-types-of-virtual-reality/ [https://perma.cc/RAT9-LUD9].

[115] GRIGORE BURDEA & PHILLIPE COIFFET, VIRTUAL REALITY TECHNOLOGY 2 (2d ed. 2003). Burdea and Coiffet go on to describe other key characteristics of the technology. They also discuss a third "I" characteristic of IR— its use of the user's imagination. *Id.* at 3.

[116] Stefano Scheggi et al., *Touch the Virtual Reality: Using the Leap Motion Controller for Hand Tracking and Wearable Tactile Devices for Immersive Haptic Rendering*, SIGGRAPH '15 (July 2015), https://dl.acm.org/doi/pdf/10.1145/2787626.2792651; C. Loscos et al., *The Museum of Pure Form: Touching Real Statues in an Immersive Virtual Museum*, VAST (2004), https://diglib.eg.org/bitstream/handle/10.2312/VAST.VAST04.271-279/271-279.pdf?sequence=1&isAllowed=n.

[117] A. Pilacinski, M. Metzler & C. Klaes, *Phantom Touch Illusion, An Unexpected Phenomenological Effect of Tactile Gating in the Absence of Tactile Stimulation*. SCI. REP. 13, 15453 (2023); *see, e.g.*, Madelaine Ley & Nathan Rambukkana, *Touching at a Distance: Digital Intimacies, Haptic Platforms, and the Ethics of Consent, Science and Engineering Ethics*, SCI. & ENG'G ETHICS (Sep. 21, 2021) (discussing the impact of haptic technology).

provide real-time renderings to create the illusion of interaction with a built environment and with other users in it, in real time.[118]

The COVID-19 pandemic generated unanticipated proof-of-concept for how these technologies might find general adoption. Tellingly, the social media and interactive gaming realms of the metaverse—tapping into the same network dynamics and frictionless sign-ups that had enable non-immersive social media's explosive growth in the preceding decade—grew most.[119] Interest in virtual interaction surged as restrictions on in-person events and concern over viral transmission made connecting with others without leaving home more attractive than ever. Roblox saw a 40% increase in users in March 2020 alone and by April 2020, two-thirds of all U.S. children 9-12 years old were using Roblox.[120]

Platforms hustled to expand offerings that met the need for means of social interaction, commerce, education, and professional service delivery under circumstances in which physical mobility or face-to-face gathering was risky or even banned. "Epic Games' popular free-to-play title Fortnite has shown that people, especially kids, are willing to flock to attractive virtual spaces to hold meetups and parties as ways to socialize during the pandemic," explained one reporter in July 2020, adding that in turn, Roblox was creating "its own private space for [people] to host virtual private birthday parties and social gatherings."[121]

---

[118] *See* Janna Anderson & Lee Rainie, *The Metaverse in 2040*, PEW RSCH. CTR. (June 30, 2022), https://www.pewresearch.org/internet/2022/06/30/the-metaverse-in-2040/ [https://perma.cc/G7GK-R8MQ].

[119] Kevin Westcott, Chris Arkenberg, Jana Arbanas, Brooke Auxier, Jeff Loucks & Kevin Downs, *2022 Digital Media Trends, 16th Edition: Toward the Metaverse*, DELOITTE (Mar. 28, 2022), https://www2.deloitte.com/us/en/insights/industry/technology/digital-media-trends-consumption-habits-survey/summary.html [https://perma.cc/F6SL-FM79].

[120] Taylor Lyles, *Over Half of US Kids are Playing Roblox, and It's About to Host Fortnite-esque Virtual Parties Too*, VERGE (July 21, 2020), https://www.theverge.com/2020/7/21/21333431/roblox-over-half-of-us-kids-playing-virtual-parties-fortnite [https://perma.cc/VK42-5QS6].

[121] *Id.*

Roblox went public in March 2021 with a valuation of $42 billion. By December 2021, driven by what headlines called "metaverse mania," its stock value reached $68 billion.[122] In keeping with the pattern described above, this building-out of virtual spaces within the Roblox platform advanced through a mix of company-generated, voluntary user-generated, and commercial developer-generated coding.[123] As of 2022 roughly "1.3 million creators were earning" exchangeable in-platform currency from their work, "on track to earn $500 million that same year."[124]

Uncoincidentally, in the wake of this pandemic-era proof-of-concept—with the sales figures and investments it occasioned still rising—Facebook chose to rename itself Meta and hustled to launch its own game app, Horizon World, which it hoped would leverage Facebook's massive user base to establish itself as the default front door of the metaverse.[125] Horizon Worlds provides a digitally engineered environment structure that others (both commercial providers and individual users) can build upon to create their own interactive settings. [126] Other platforms currently accessible by IR technology include (as of November 2024) Roblox, Fortnite,

---

[122] Natasha Dailey, *Roblox Has Added Nearly $26 billion to its Market Cap as Metaverse Mania Pushes its Value Past Brands like FedEx and Ferrari,* BUS. INSIDER (Dec. 8, 2021), https://markets.businessinsider.com/news/stocks/roblox-more-valuable-than-fedex-ferrari-amid-metaverse-mania-2021-12 [https://perma.cc/GCZ4-VTGL].

[123] *See e.g.*, Jenn Brice, *Roblox Boosts Developer Payouts in New Plan to Supercharge Growth*, FORTUNE (Sept. 7, 2024), https://fortune.com/2024/09/07/roblox-game-developers-revenue-share-paid-tiers-conference/ [https://perma.cc/Y9LF-B6GA].

[124] Joseph Cox, *How Roblox 'Beamers' Get Rich Stealing from Children*, VICE (Feb. 14, 2022), https://www.vice.com/en/article/88gd4a/roblox-beaming-hackers [https://perma.cc/TEG5-4KEP].

[125] Josh Constine, *Facebook Announces Horizon, a VR Massive-Multiplayer World*, TECHCRUNCH (Sept. 25, 2019), https://techcrunch.com/2019/09/25/facebook-horizon/ [https://perma.cc/M9GN-ZQB8].

[126] *Id.*

Minecraft, Decentraland, Sandbox, and Second Life.[127] Horizon Worlds seems to be struggling to hold onto 200,000 or so monthly users,[128] Second Life has about 750,000 monthly users,[129] and Roblox dwarfs all the others with over 50 million active daily users worldwide.[130]

In sum, "the metaverse" is neither ineffable nor a seamless realm, despite builders' eagerness to promote that illusion. Rather we have a stack of tech products and creators, of widely varying size and permanence, building the hardware, platforms, and code that support individual IR instances, with varying possibilities for action and interaction built into each instance.[131] Some instances will be platform-generated, some user-generated, and others built by professionals for individuals or corporate third parties.[132] These differences matter, because patterns of predictable harm—and possibilities of legal redress—will vary systematically across these different realms, as we detail in Part II.

Some stretches of the metaverse (including those built by

---

[127] *See, e.g.*, *How Metaverse Gaming is Changing the Virtual World?,* POLARIS MARKET RSCH. (Nov. 19, 2024), https://www.polarismarketresearch.com/blog/top-names-to-invest-in-the-metaverse-gaming-2025.

[128] Jonathan Vanian, *Meta is Rebooting Horizon Worlds as the VR Platform Struggles to Grow*, CNBC (July 28, 2023), https://www.cnbc.com/2023/07/28/meta-horizon-worlds-metaverse-is-getting-an-update-with-more-games.html [https://perma.cc/7ELJ-HXE5].

[129] *Original Metaverse Second Life Celebrates 20th Birthday*, BUS. WIRE (June 22, 2023), https://finance.yahoo.com/news/original-metaverse-second-life-celebrates-130000976.html.

[130] David Curry, *Roblox Revenue and Usage Statistics (2024)*, BUS. OF APPS (Jan. 8, 2024), https://www.businessofapps.com/data/roblox-statistics/ [https://perma.cc/Z6ZS-AVL7].

[131] Alex Heath, *Meta's Social VR Platform Horizon Hits 300,000 Users*, VERGE, (Feb. 17, 2022), https://www.theverge.com/2022/2/17/22939297/meta-social-vr-platform-horizon-300000-users; Jay Peters, *Roblox is Coming to Meta's Quest VR Headsets*, VERGE (July 12, 2023), https://www.theverge.com/2023/7/12/23792594/roblox-meta-quest-2-3-pro-vr-headsets [https://perma.cc/JV8C-SSGZ].

[132] One example would be an auto manufacturer who wants to have a virtual showroom where users can "try out" different models by "driving" them. *See* discussion *infra* Section II.D.

Meta) are pursuing a pure "audience monetization" model, in which users create free accounts to access a seemingly free service and engage with platforms without paying a monetary fee to access the content. Under this framework, just like on social media platforms, the users *become* the product: the "data exhaust" produced by their movements through the platform is either used by the technology company itself or sold to third-party vendors who then mine the data points for various ends, such as targeted advertising.[133]

As noted above, this has been the dominant type of commercialization chosen by social media companies over the past decade. This is the strategy reflected, for instance, in Horizon Worlds' description of how one core category of instances on its platform—what Meta is calling "members-only worlds"—are intended to work:

> Members-only worlds are a new type of closed space, similar to personal space, that is membership-based, where communities of like-minded people can come together and enjoy a shared experience. World creators and admins, if assigned to the world by a creator, are responsible for governance in this space and can select members to join their world. Only creators can set additional world-specific rules for their members-only world.[134]

---

[133] Shoshana Zuboff, *Big Other: Surveillance Capitalism and the Prospects of an Information Civilization*, 30 J. INFO. TECH. 75–89 (2015). One of us has written extensively on this type of interface and its potential legal consequences (particularly around the laws of data privacy). For a list of these laws see Jena Martin, *Data Privacy Issues in West Virginia and Beyond: An Overview*, (2nd Edition White Paper), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4896449. Ironically, in the particular scenario that we are talking about in *this* Article, data privacy could actually be used as a shield for malfeasant tortfeasors, which is a challenge we explore in Section III.B.

[134] *Members-Only Worlds in Meta Horizon Worlds*, META, https://www.meta.com/help/quest/articles/horizon/explore-horizon-

Other financial models are possible, with different implications for platform design, user experience, and prevalence of harms. For instance, platforms could charge users to access the platform. This is the model of the long-established virtual world, Second Life. As its founders explain, explicitly contrasting their model to Meta's, "[w]e spend so much more money per person on the Second Lifers, on the residents."[135] This approach is part of what has kept Second Life's growth modest, they note, with users hovering around one million rather than the hundreds of millions on the large gaming platforms, or the 3 billion who used Facebook worldwide in 2023.[136] But it is also part of what has allowed Second Life to eschew the pursuit of addictive design. As the founders explain, "if advertising is your business model, you want everybody in there all the time. You want to spend as little money as you can supporting them, and you want to get as much money as you can through volume."[137] Second Life's core customers are its users, and it works to keep them happy; Facebook's core customers are its advertisers, and it works to keep them happy. Hybrid monetization schemes also abound; many IR games currently offer both basic free and enhanced subscription-based alternatives. Gaming platforms often feature "ubiquitous microtransaction design," which continuously "nudges players to purchase in order to maximize

---

worlds/members-only-worlds/. For the moment, instances of this kind are restricted to a total of 150 members and to a maximum of 25 in the world at any one time and are limited to users 18 and older. *Id.* On how ease of account creation leads to the massive presence of deceptive "users" in virtual worlds, see Emma Roth, *Roblox Accused of Lying to Investors About User Numbers by Hindenburg Research*, VERGE (Oct. 8, 2024) https://www.theverge.com/2024/10/8/24265145/roblox-hindenburg-reseach-dau-child-safety-short-seller-report; *Metaverse Security: Emerging Scams and Phishing Risks*, PWC https://www.pwc.com/us/en/tech-effect/cybersecurity/emerging-scams-and-phishing-risks-in-the-metaverse.html [https://perma.cc/Z6GY-2YTX].

[135] Tyler Wilde, *The Creator of Second Life Has a Lot to Say About All These New Metaverses*, PCPC GAMER (Apr. 1, 2022), https://www.pcgamer.com/second-life-metaverse-interview/ [https://perma.cc/TYK5-H2VS].

[136] *Id.*

[137] *Id*.

profit."[138]

These monetization models stand in contrast to the financial structures that undergird business use-cases of the metaverse, including advertising and sales, internal communications, and manufacturing. Businesses' metaverse ventures for retail and advertising will be built and maintained either by contractors or in-house employees, in either case paid for by the corporation whose goods are being promoted. In turn, enterprise uses for internal communications will likely rely on a freemium/paid premium subscription model, as do teleconferencing services like Zoom and Slack, or perhaps eventually be incorporated into standard enterprise software suites and bundled into licenses similar to Microsoft offerings.[139]

The retail industry has already begun to reap profits from the use of IR in sales.[140] For example, when the pandemic significantly curtailed face-to-face interactions, corporations began pivoting to in-home shopping experiences that simulated in-store shopping, including allowing customers to try on clothes, see how furniture would look in their home, and speak with a sales associate.[141] Those buying clothes benefit from

---

[138] Yubo Kou & Xinning Gui, *Harmful Design in the Metaverse and How to Mitigate it: A Case Study of User-Generated Virtual Worlds on Roblox*, *in* DIS '23: PRO. 2023 ACM DESIGNING INTERACTIVE SYS. CONF. 175 (May 2023), https://doi.org/10.1145/3563657.3595960 [https://perma.cc/HM5W-JBTR].

[139] Seufert, Freemium Economic, *supra* note 107; Kate Whiting, *Consumer, Enterprise or Industrial? The 3 Main Ways We Are Using the 'Metaverse' Explained*, WORLD ECON. F. (Feb. 17, 2023), https://www.weforum.org/agenda/2023/02/metaverse-use-cases-industrial-consumer-enterprise/; WORLD ECON. F., DEMYSTIFYING THE CONSUMER METAVERSE 25 (Jan. 2023), https://www3.weforum.org/docs/WEF_Demystifying_the_Consumer_Metaverse.pdf*; see also* WORLD ECON. F., INTEROPERABILITY IN THE METAVERSE (Jan. 2023), https://www3.weforum.org/docs/WEF_Interoperability_in_the_Metaverse.pdf.

[140] *Id.*

[141] *See* Serenity Gibbons, *How Businesses Are Using VR to Survive the*

haptic technology which allows them to feel the fabric; those buying cars benefit from auditory and visual interfaces that allow them to see and hear the automobile.[142]

Enterprise use cases include trainings and onboardings, meetings and events, and can include using gamification to help users train for physical tasks.[143] The securities industry already uses aspects of the IR technology to train its employees in aspects of trading.[144]

Finally, as the World Economic Forum suggests, industrial applications will allow IR technology to create spaces that permit individuals to manipulate physically distant objects with great precision.[145] For instance, using this technology, doctors could guide microscopic surgeries, in real time, via immersive

---

Covid-19 Era, FORBES (May 2, 2020) (discussing how companies increased their use of AR to increase retail engagement and sales), https://www.forbes.com/sites/serenitygibbons/2020/05/02/how-businesses-are-using-vr-to-survive-the-covid-19-era/ [https://perma.cc/LL78-QQJN]; Helen Papagiannis, *How AR is Redefining Retail in the Pandemic,* HARV. BUS. REV. (Oct. 7, 2020) (stating "Augmented Reality (AR) applications have been on the rise with virtual "try-before-you-buy" experiences ranging from previewing furniture and products in your home with everyday brands like IKEA and Home Depot, to virtually trying on luxury fashion such as Louis Vuitton and Gucci"), https://hbr.org/2020/10/how-ar-is-redefining-retail-in-the-pandemic [https://perma.cc/UJX3-39LD].

[142] Bernard Marr, *10 Best Examples of Augmented and Virtual Reality in Retail*, FORBES (Sept. 13, 2021), https://www.forbes.com/sites/bernardmarr/2021/09/13/10-best-examples-of-augmented-and-virtual-reality-in-retail/?sh=1ac51366269d [https://perma.cc/XY9C-VVTL].

[143] DEMYSTIFYING THE CONSUMER METAVERSE, *supra* note 139.

[144] *See, e.g.*, *Augmented Reality Becomes a Reality for Trading*, TRADERS MAG. (Oct. 1, 2017), https://www.tradersmagazine.com/departments/technology/augmented-reality-becomes-a-reality-for-trading/ [https://perma.cc/7A5V-WBUG]; Richard van Hooijdonk, *How Immersive Technology is Revolutionising the Financial Services Industry*, RICHARD VAN HOOIJDONK.COM (June 9, 2022), https://blog.richardvanhooijdonk.com/en/how-immersive-technology-is-revolutionising-the-financial-services-industry/ [https://perma.cc/KWH4-PBVN].

[145] *See supra* note 139.

3D rather than 2D visual imaging.[146]

In sum, the new technologies and platforms will offer innovative and creative ways for consumers or employees to engage with corporations, products, and each other. But as with any new avenue of interaction, new possibilities of harm will likewise ensue. In this next Part, we discuss three broad categories of harms and provide specific examples of how they may be actualized.

II. Predictable Harms in the Metaverse

The harms that will result in the metaverse are both painful and predictable. Moreover, they will be borne primarily by individuals. Many of these harms are clearly analogous to crimes or civil violations that are routinely committed and adjudicated in the physical world.[147] However, because of the varied monetization models discussed above, the possibilities of legal redress or remediation will diverge.

In business-sponsored interactions in the metaverse, we expect existing structures for accountability to be sufficient to provide redress. In contrast, in the social media and interactive gaming realms of the metaverse, we predict that the prevalence of anonymous and ephemeral third parties will systematically create novel dilemmas of policing and redress. Both the accelerated pace of harm-doing and the shielding effects of the "veil of scale" mean that when crimes are committed in cyberspace, accountability for the tortfeasors themselves may be vanishingly rare. Meanwhile, the platforms will predictably

---

[146] Analysts suggest Augmented Reality (rather than Virtual Reality) will be most relevant for such "industrial" metaverse use cases. Peggy Johnson, *3 Shared Principles to Maximize the Value of the Metaverse*, WORLD. ECON. F. (Jan. 18, 2023), https://www.weforum.org/agenda/2023/01/davos23-3-shared-principles-to-maximize-the-value-of-the-metaverse/ ("AR ultimately has the greatest potential. With AR, you can still interact with the objects, tools, environments, and people around you – making adoption easier, providing greater value to existing activities and speeding the path to Return on Investment.").

[147] Christopher DiMatteo & Karine Russell, *The Metaverse: Litigation Implications*, BLAKES (Dec. 8, 2022), https://www.blakes.com/insights/trends/2022/the-metaverse-litigation-implications [https://perma.cc/G3GR-HS3T].

argue that as interactive computer service providers, they are shielded by Section 230 from being treated as publishers or speakers of content generated by others—in this case, those ephemeral bad actors. However, as we discuss below, such a simplistic application of Section 230 would obstruct the full accounting and allocation of the costs of platform-enabled harms in the social metaverse.

The following Sections will discuss different use cases of the metaverse, and how lines of legal accountability can be drawn if there is any harm.

A. The Metaverse as Corporate Showroom

Many of the commercial use cases proposed for the metaverse utilize a virtual environment to prototype or showcase a product or provide training in a skill that will later exist or be employed "in real life." We refer to this as the "corporate showroom."

In this Section, we consider predictable harms that may occur when companies seek to use the metaverse as a corporate showroom, and argue that however novel the circumstances, existing legal structures will be able to handle novel harms when dealing with a visible and fixed bad actor.

Let's consider a first category of harm: It Didn't Work in Real Life. What happens if consumers use IR to design a car, but when they drive the car in real life, they discover a fundamental flaw that leads to harm? Who should be liable? For instance, if the car that BMW sold you using its virtual showroom ends up being significantly altered when it arrives at your front door, then presumably a cause of action would arise under a breach of contract claim, and a consumer could use promissory estoppel theories.[148]

---

[148] Sheldon, *infra* note 157, discusses theories of promissory estoppel but in a slightly different way—he opines on issues of promissory estoppel for transactions that occur entirely within the metaverse. In contrast, we recognize that some mixed modality transactions could also lead to claims of promissory estoppel. Although we have been unable to find any case where this claim has been made, we suspect that it is only a matter of time.

Similarly, in the not-so distant future, a car mechanic could use a form of IR technology to interact with a consumer's car, diagnose the issue and then "fix it" (if the issue is software related). But what happens if his work does not actually repair the car and a harm results? Similar cases could arise regarding enterprise use. For instance, what happens if a securities trader claims that the interface used for IR training had some feature that led them to make costly mistakes when trading in real life?[149]

Finally, one potential issue may come from the false confidence that people may have from using immersive technology. For instance, many surgeons are now using IR to hone techniques before they work on real patients.[150] But what happens if the technology gives the surgeons false confidence? The current practices of some surgeons may already be a harbinger of these types of claims. For instance, in October 2023, the *New York Times* reported that there was an increase in botched hernia repair surgeries that seem to correlate with surgeons "watching videos [on the subject] on social media."[151] The *Times'* investigation found that "one out of four surgeons said they taught themselves how to perform the [complex] operation by watching Facebook and YouTube videos."[152]

Nevertheless, as long as there is a fixed and identifiable

In the interim, perhaps the most relevant real-life analogy occurs within the realm of art and purchases of "exhibition" copies of famous works. For a discussion of the issue, see Amy Adler, *Artificial Authenticity,* 98 N.Y.U. L. REV. 706, 734-35 (2023).

[149] For an extreme example of harms in this category, consider the field of explosive ordinance disposal (EOD). If contractors in a private security realm use augmented reality to learn the nuances of bomb diffusion, and it turns out the bomb design was different in real life, then the consequences could be devastating.

[150] Tristan Greene, *Doctors Turn to Apple Vision Pro Headset to Practice Surgery Amid Cadaver Shortage*, COINTELEGRAPH, (Apr. 17, 2024), https://cointelegraph.com/news/doctors-apple-vr-ar-mr-virtual-reality-vision-pro-headset-practice-surgery-cadaver-shortage.

[151] Sarah Kliff & Katie Thomas, *How a Lucrative Surgery Took Off Online and Disfigured Patients*, N.Y. TIMES (Oct. 30, 2023), https://www.nytimes.com/2023/10/30/health/hernia-surgery-component-separation.html.

[152] *Id.*

individual or corporate entity making the promise, we should expect our existing legal constructs (likely those based in either tort or breach of contract claims) to be smoothly capable of sanctioning harm, making victims whole, and incentivizing better behavior.

Not so in the stretches of the metaverse that follow the social media business model and approach to monetization.

This distinction comes to the fore clearly in consideration of another category of potential risks in the metaverse: ownership disputes around digital creations. As we discuss below, such disputes will arise in both the business-sponsored metaverse and the social model/free-to-play gaming modelled metaverse realms, thereby providing a lens from which to analyze the inadequacy of the current legal structure in redressing harms that stem from the latter.

B. Ownership Rights in the New Metaverse

Grappling with ownership of intangible objects is not a new challenge; the field of intellectual property exists solely as an attempt to deconstruct, analyze, and examine how to attribute ownership to intangible creations.[153] For instance, arts and entertainment are already the subject of significant copyright and intellectual property issues.[154] Indeed, as recently as May 2023, the Supreme Court was addressing such questions in the case of *Warhol v. Goldsmith*.[155] Many of these issues concern

---

[153] *See, e.g.,* Justin Hughes, *The Philosophy of Intellectual Property*, 77 GEO. L. J. 287, 294 (1988) (discussing the philosophical underpinnings of intellectual property law).

[154] For instance, one of the most significant issues that the entertainment field has faced in modern times is the rise of digital piracy, which was once only capable in the hands of a few, but is now easily deployed by most consumers. For a relatively early clarion call of the issue, see Girjesh Shukla, *Copyrights Piracy in Entertainment Media: Technological Development and Challenges to the Intellectual Property Rights*, (May 18, 2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1845278 [https://perma.cc/MAF6-2G9Z].

[155] Andy Warhol Found. for the Visual Arts, Inc. v. Goldsmith, 598 U.S. 508 (2023). For a discussion of the implication and potential consequences of the case, see Caroline Osborne & Stephen Wolfson, Andy Warhol Foundation for the Visual Arts, Inc. v. Goldsmith*, a Narrow Rule or a Transformation Decision? An Essay*, 84 OHIO ST. L.J. ONLINE 1 (2023).

who owns the intellectual property, and (as in the case of the *Warhol* decision) who may appropriate the source material to create new art. As one author notes, "[s]ince the domain of intellectual property rights is not some tangible object but the fruits of a person's thoughts and brainpower, they should logically operate in much the same way in the metaverse as in the real world." [156] Yet even within our current analog environment, unpacking "ownership" within this context is often incredibly complicated. In the metaverse, these issues will likely be exacerbated.[157]

For instance, if someone creates a piece of art within the metaverse, does its intangible nature make its ownership interest more amorphous? Early prognosticating by practitioners would seem to indicate that it would not. [158] However, others disagree, stating that providing these things within the metaverse may make protection difficult.[159]

---

[156] Aanya Sharma, *Intellectual Property Rights in the World of NFTs and the Metaverse*, 3 JUS. CORPUS. L.J. 126, 134 (2022).

[157] At least one scholar prognosticated on potential ownership issues within a virtual space before the current iteration of the metaverse was developed. Writing in 2007, David Sheldon discussed ownership issues that might emerge within the metaverse's precursor: massive multiplayer online games. As Sheldon writes, "Participants make sizable investments of social, human, and economic capital in these virtual worlds, often with the questionable expectation that the items they have collected and creations they have developed are their property." David Sheldon, Comment, *Claiming Ownership but Getting Owned: Contractual Limitations on Asserting Property Interests in Virtual Goods*, 54 UCLA L. REV. 751, 751 (2007). For further fulsome analyses of property rights in virtual worlds, see Joshua A.T. Fairfield, *Virtual Property*, 85 BOS. U. L. REV. 1047 (2009); and Joshua A.T. Fairfield, *The End of the (Virtual) World*, 112 W. VA. L. REV. 53 (2009).

[158] Stuart Irvin, Adrian Perry, Marie Lavalleye & Phil Hill, *Brands in the Metaverse Will Fight Old Battles on New Ground*, BLOOMBERG L. (Feb. 18, 2022), https://news.bloomberglaw.com/tech-and-telecom-law/brands-in-the-metaverse-will-fight-old-battles-on-new-ground [https://perma.cc/G5QL-E7D9].

[159] João Marinotti, *Can You Truly Own Anything in the Metaverse? A Law Professor Explains How Blockchains and NFTs Don't Protect Virtual Property*, CONVERSATION (Apr. 21, 2022), https://theconversation.com/can-you-truly-own-anything-in-the-metaverse-a-law-professor-explains-how-blockchains-and-nfts-dont-protect-virtual-property-179067 [https://perma.cc/NNG5-3HPK].

Now imagine that there is an analog equivalent for this intangible good. Does the adaptation of an existing physical object from its virtual space sufficiently transform it to have it fall outside the bounds of the protections of intellectual property law?[160] Conversely, if someone created a work of art in the analog world and then wanted to display this work of art within a virtual space, the owner could have concerns about the online facsimile being forged. While non-fungible tokens (NFTs)[161] can mitigate this issue, forgeries and disputes could still happen. Although intellectual property law theoretically provides some redress,[162] the ephemeral nature of the metaverse can make remediation unlikely. For instance, does the current stage of technology provide for a marker relating to who *originated* the intellectual property? If not, then it would be difficult for a court to decide who created two identical pieces that were forged specifically within the

---

[160] Torsten M. Kracht & Daniel A. Schultz, *What Kinds of Issues Are Being Litigated Related to the Metaverse and NFTs?*, LEGALTECH NEWS (Apr. 11, 2023), https://www.law.com/legaltechnews/2023/04/11/what-kinds-of-issues-are-being-litigated-related-to-the-metaverse-and-nfts/?slreturn=20241130163503 [https://perma.cc/68TP-MZV5].

[161] As one author notes, "NFTs are essentially unique tokens that provide authentic and verifiable proof of ownership over an asset, containing the metadata associated with the asset encoded within a smart contract that forms part of the NFT. The copy of the asset/artwork is included within the NFT through a link or a digital copy." Sharma, *supra* note 156, at 129.

[162] Irvin, *supra* note 158. Although, even then, the redress would likely only be limited to the person who has forged the IP itself and not to the platform that hosted the site where the forgeries occur. The high standard enunciated by courts would likely prevent secondary liability from being attached to online marketplaces that merely hosted the platform on which the counterfeit product was sold—even if they had general knowledge that forgeries were being sold within that marketplace. *See, e.g.*, Tiffany Inc. v. eBay, Inc., 600 F.3d 93, 107 (2d. Cir. 2010) (holding that secondary liability couldn't be attached to eBay for trademark infringement claims based on eBay's generalized knowledge of counterfeit goods being sold on its "online marketplace"). For discussions among scholars regarding secondary liability within IP after the *Tiffany* decision, see Mark P. McKenna, *Probabilistic Knowledge of Third-Party Trademark Infringement*, 2011 STAN. TECH. L. REV. 10 (2011); Elizabeth K. Levin, Note, *A Safe Harbor for Trademark; Reevaluating Secondary Trademark Liability after* Tiffany v. eBay, 24 BERK. TECH. L. J. 491 (2009).

metaverse. In addition, as one author notes, "[s]ince these creative works are now increasingly being dealt with in the form of NFTs, it begs the question of which of these rights, if any, get transferred to the buyer when they buy an NFT which represents some kind of art or creation."[163] Further legal challenges arise when someone who is not the owner of the source material within the analog world nonetheless creates an NFT of the material and then sells it to a person within the metaverse. Who has ownership of the NFT in that instance? The creator of the source material? The creator of the NFT? Or the purchaser of the NFT from the NFT's creator?

While this discussion of NFTs has been framed as a matter of future hypotheticals, theft of intangible but valuable property already exists as an endemic phenomenon within several of the virtual worlds, such as Roblox.[164] When the intellectual property at stake is as valuable as the rights to Andy Warhol's image, and when those seeking to own and profit from it are established corporate actors, one can trust that litigation will be pursued directly against those actors, with no need for novel theories of platform responsibility. But the vast majority of ownership disputes and intellectual property theft in the metaverse will look more like the theft of user-produced content by hackers within Roblox, which already sometimes add up to thousands or tens of thousands of dollars.[165] This endemic phenomenon rarely gains public attention precisely because it is quotidian, carried out in virtual spaces, and often uses hosting sites spread across international jurisdictions, disrupting legal remedies.[166]

These are, of course, exactly the conditions that will

---

[163] Sharma, *supra* note 156, at 130.

[164] Cox, *supra* note 124.

[165] *See, e.g.*, Doe v. Roblox Corp., 602 F.Supp.3d 1243 (N.D. Cal. 2022) (allowing a lawsuit against Roblox for failing to reimburse purchasers—in this case, children—when user-made items they have purchased in game are subsequently judged, by Roblox, violative of game standards).

[166] *See* Cox, *supra* note 124 ("The owner of RBX.Flip, the gambling site, previously told RoZone that Roblox sent a legal demand to Amazon Web Services and their subsequent host, which both took the site down. RBX.Flip then moved to another 'offshore' host 'who doesn't really care' about the DMCA copyright law, they said.").

characterize the social media/interactive gaming-driven metaverse, and in the following Section, we will discuss how routes to accountability in this emerging metaverse are hampered by the "veil of scale."

C. The Metaverse as Social Media on Steroids Could be a Victimizers' Paradise Under Current Jurisprudence

Unlike the metaverse-as-corporate-showroom, the social media and interactive gaming-driven spaces within the metaverse will be powered by the lure of third-party interaction and beset by third-party harms. Direct application of Section 230 precedents will be tempting here, because the core elements that trigger Section 230's liability shield will seem to be present. The three-prong test laid out in *Barnes v. Yahoo!, Inc.* in 2009, and routinely applied to social media companies since then, asks: 1) is the defendant a provider of an interactive computer service, and 2) does the suit seek to treat them as publisher or speaker of 3) content generated by someone else?[167] Answering those questions in the affirmative would leave metaverse platform-providers shielded from liability. But, what about the third parties directly responsible for harms? They in turn will be shielded by the "veil of scale" that those same platform-providers created.

Some harms that will fall into this accountability gap could be considered "intangible," similar to the psychological harms caused by witnessing something traumatic. However, the harm cannot simply be equated to visual exposure in the analog

---

[167] Barnes v. Yahoo!, Inc., 570 F.3d 1096, 1100-01 (9th Cir. 2009). For adoption by other circuits, *see e.g.*, Jane Doe No. 1 v. Backpage.Com, LLC, 817 F.3d 12, 19 (1st Cir. 2016); Marshall's Locksmith Serv. Inc. v. Google, LLC, 925 F.3d 1263, 1267-68 (D.C. Cir. 2019); and Federal Trade Commission v. LeadClick Media, LLC, 838 F.3d 158, 173 (2d Cir. 2016). More broadly, see discussion of standard lower court use of the *Barnes* test in an amicus brief presented in *Gonzalez v. Google*, (U.S. 2023). Brief of the Cato Institute, R Street Institute, and Americans For Tax Reform as Amici Curiae Supporting Respondent, Gonzalez v .Google, Case 598 U.S. 617 (2023) (No. 21-1333). Ultimately, the Supreme Court did not rule on the adoption of this test, instead remanding the case for reconsideration in light of the new *Twitter v. Taamneh* decision under which "the plaintiffs' complaint—independent of § 230—states little if any claim of relief." Gonzalez v. Google, LLC, 598 U.S. 617, 622 (2023).

world. For instance, being placed in an immersive experience where your avatar is being assaulted, while not the same as being assaulted in real life, would likely be considered a more invasive experience then watching a video of your avatar being assaulted.[168] The haptic features that are already a part of IR models would likely intensify the distinction.[169]

Such harms, however, are not our main focus.

Not all harmful encounters within the metaverse require a theory treating immersive virtual experience as real-world suffering in order to be crimes. We are thinking first and foremost of a grimly prevalent category of criminal action that can be executed with no need for physical presence, one that has been radically enabled by the access that social media and smartphone cameras provide: the sexual solicitation of children.[170]

The consumption by adults of pornographic images of consenting adults is neither itself illegal, nor necessarily a reflection of a prior crime (although available evidence suggests that some pornography available on the internet was

---

[168] For a detailed, first-person account of such an IR assault, see Katherine Singh, *There's Not Much We Can Legally Do About Sexual Assault In The Metaverse*, REFINERY29 (Jun. 9, 2022), www.refinery29.com/en-us/2022/06/11004248/is-metaverse-sexual-assault-illegal [https://perma.cc/J9S8-67NQ]; *see also* Laurie Clarke, *Can We Create a Moral Metaverse?*, GUARDIAN (May 14, 2022), https://www.theguardian.com/technology/2022/may/14/can-we-create-a-moral-metaverse.

[169] For an earlier wave of scholarship on whether, for instance, an assault by an avatar on an avatar that contravenes in-game rules should be legally cognizable in some way, see Kerr, *supra* note 3; Balkin, *supra* note 3; Hunter & Lastowka, *supra* note 3; Chin, *supra* note 3; and Smyth, *supra* note 3.

[170] *See* Chad M.S. Steel, Emily Newman, Suzanne O'Rourke & Ethel Quayle, *An Integrative Review of Historical Technology and Countermeasure Usage Trends in Online Child Sexual Exploitation Material Offenders*, 23 FORENSIC SCI. INT'L: DIGIT. INVESTIGATION 300971 (June 2020); Victoria Baines, *Online Child Sexual Exploitation: Towards an Optimal International Response*, 4 J. CYBER POL. 197-215 (2019); Michael H. Keller & Gabriel J.X. Dance, *The Internet Is Overrun With Images of Child Sexual Abuse. What Went Wrong?*, N.Y. TIMES (Sept., 29, 2019), https://www.nytimes.com/interactive/2019/09/28/us/child-sex-abuse.html.

produced under conditions of coercion).[171] In contrast, not only is the solicitation, possession, sale, or exchange of photographic or video images of children in sexually suggestive contexts, or involved in sexual acts of any kind, itself criminal, but the creation of every such image itself was predicated on an act of sexual abuse.[172] This is true even if the interaction through which the images were produced took place via purely online interaction.[173]

It is sometimes imagined that child sexual exploitation is confined to hidden corners of the "dark web," and that platforms like Facebook and Instagram are not part of this problem. On the contrary, online predators use public virtual spaces to meet children who they then seek to peel off into one-on-one interactions.[174] Experts find that initial contact often happens on one platform with crimes committed elsewhere on private messaging channels.[175] Again, this risk is the opposite

---

[171] *See, e.g.*, Bianca Bruno, *Women Win $13 Million in GirlsDoPorn Fraud Suit*, COURTHOUSE NEWS SERV. (Jan. 2, 2020), https://www.courthousenews.com/women-win-13-million-in-girlsdoporn-fraud-suit/.

[172] The exception to this latter point is CSAM generated by AI tools, which involves no actual child in its production. While the creation, possession, and exchange of AI generated CSAM is illegal in the U.S. as in many other countries, its generation does not require the additional crime of sexual solicitation or assault. Riana Pfefferkorn, *Addressing Computer-Generated Child Sex Abuse Imagery: Legal Framework and Policy Implications*, LAWFARE (Feb 5. 2024, 5:01 AM), https://www.lawfaremedia.org/article/addressing-computer-generated-child-sex-abuse-imagery-legal-framework-and-policy-implications.

[173] *See* 18 U.S.C. §§ 2242, 2252A, as well as similar state laws.

[174] *See* Lara Putnam, *Child Endangerment in "Los Picus" Fan Groups: Facebook (Still) Has a Child Predation Problem*, TECH POLICY PRESS (Jan. 23, 2024) (describing the issue and the dangers), https://www.techpolicy.press/child-endangerment-in-los-picus-fan-groups-facebook-still-has-a-child-predation-problem/ [https://perma.cc/K9RS-3SUK] and Putnam, *Latin America's Children at Risk*, *supra* note 76.

[175] *See, e.g.*, Baines, *supra* note 170; Steel et. al., *supra* note 170; Jeff Horwitz & Katherine Blunt, *Meta Is Struggling to Boot Pedophiles Off Facebook and Instagram*, WALL ST. J. (Dec. 1, 2023), https://www.wsj.com/tech/meta-facebook-instagram-pedophiles-enforcement-struggles-dceb3548; Jeff Horwitz & Katherine Blunt, *Instagram Connects Vast Pedophile Network*, WALL. ST. J. (June 7, 2023), https://www.wsj.com/articles/instagram-vast-pedophile-network-4ab7189.

of rare: "Two-thirds of minors reported they have been asked by someone they met online to move from a public forum to a private conversation on a different platform."[176] Extensive reporting in the past several years has shown how virtual spaces including gaming, Roblox, Instagram, and Facebook have all become targets for grooming and exploitation.[177]

Notably, the interactive gaming sites that Silicon Valley entrepreneurs and investors expect to be a main draw of users into the metaverse are exactly the sites currently serving as this kind of risky "front door" for the interactions through which grooming, predation, and extortion can start. Among *all* children aged 9 to 12 surveyed in a representative U.S. sample—not just among those who are users of the following platforms—eighteen percent report they exchange messages *daily* on Roblox with someone they do not know in person.[178] Seventeen percent of all surveyed 9-12 year olds have that experience daily on TikTok; seventeen percent on Facebook Messenger; sixteen percent on Minecraft; fifteen percent on each of on Snapchat, Instagram, and Fortnite; fourteen percent on Among Us, a videogame; fourteen percent on Facebook; and fourteen percent on YouTube.[179] Relatedly, half of all minors—and two-thirds of LGBTQ+ minors—have experienced an interaction while messaging with a male over

---

[176] THORN, *Online Grooming: Examining risky encounters amid everyday digital socialization. Findings from 2021 qualitative and quantitative research among 9-17-year-olds* 4 (Apr. 2022) https://info.thorn.org/hubfs/Research/2022_Online_Grooming_Report.pdf [https://perma.cc/HG8Q-SQ8L].

[177] *See* Nellie Bowles & Michael H. Keller, *Video Games and Online Chats Are 'Hunting Grounds' for Sexual Predators*, N.Y. TIMES (Dec. 7, 2019), https://www.nytimes.com/interactive/2019/12/07/us/video-games-child-sex-abuse.html; Burt Helm, *Sex, Lies, and Video Games: Inside Roblox's War on Porn*, FAST CO. (Aug. 19, 2020), https://www.fastcompany.com/90539906/sex-lies-and-video-games-inside-roblox-war-on-porn; Horwitz & Blunt, *Meta is Struggling supra* note 175; Horwitz & Blunt, *Instagram Connects Vast Pedophile Network*, *supra* note 175; Lara Putnam, *Facebook Has a Child Predation Problem*, WIRED (Mar. 13, 2022), https://www.wired.com/story/facebook-has-a-child-predation-problem/.

[178] THORN, *Online Grooming*, *supra* note 176 at 32.

[179] *Id.*

thirty that made them uncomfortable.[180]

What are the results of this kind of expansion—at scale—of children's participation in spaces ripe for sexual endangerment? From 2021 to 2022, the National Center of Missing and Exploited Children (the official U.S. hotline and clearinghouse for such reports) "saw an astounding 82% increase in reports of online enticement of children for sexual acts."[181]

When reporter Paul Murray decided to explore Meta's Horizon Worlds, his very first conversation there was not with an adult at all. Rather, it was with one of the children with whom Murray found Horizon World was "overrun": under-13-year-olds nominally barred from using Meta's headset but doing so via a parent's or other relative's device.[182] Murray encountered a crudely-named avatar, apparently being used by a child accessing Horizon World through a headset belonging to an adult in their household. The child's first words in response to Murray's greeting described sexual harassment/solicitation the child had just experienced from another user. "'He said he wanted to eat my penis,' Nutsacksandwich says to me in a high-pitched child's voice. This is my first conversation in the metaverse."[183]

Harassment, sexual solicitation, and image-based sexual abuse by online adults have become a quotidian and expected part of the child and adolescent experience today, and the social media and online gaming platforms building the

---

[180] *Id.*

[181] THORN, EMERGING ONLINE TRENDS IN CHILD SEXUAL ABUSE (2023), https://get.safer.io/emerging-online-trends-child-safety-2023 [https://perma.cc/GP4W-CSWG].

[182] Paul Murray, *Who Is Still Inside the Metaverse? Searching for friends in Mark Zuckerberg's Deserted Fantasyland*, N.Y. MAGAZINE (Mar. 15, 2023) https://nymag.com/intelligencer/article/mark-zuckerberg-metaverse-meta-horizon-worlds.html [https://perma.cc/CES7-AY6L].

[183] *Id.* For more systematic evidence of children's presence and exposure to adult sexual content in Horizon Worlds, see Center for Countering Digital Hate, *Horizon Worlds Exposed: Bullying, Sexual Harassment of Minors, and Harmful Content are Ripe in Facebook's VR Product*, https://counterhate.com/wp-content/uploads/2023/03/Horizon-Worlds-Exposed_CCDH_0323.pdf [https://perma.cc/APE4-6JUQ].

metaverse have been ground zero for these harms. The fact that adult readers will be shocked by the words above—the kinds of interaction that 9-to 12-year olds are exposed to online routinely—underscores the scale of the problem.

D. The "Veil of Scale" as a Predator's Shield

Readers may doubt that systematic lawlessness and deception would be allowed to persist on high-profile platforms owned by publicly traded corporations like those that will build the major social media and online gaming realms of the metaverse. Surely the platforms themselves will take preventive action—or in cases of the most egregious harms, like sexual exploitation of children, law enforcement will do so?

To dispel such rosy hopes, we laid out in detail the prevalence of criminal sexual solicitation of children—leading to an explosive expansion of SG-CSAM—that is demonstrably already underway on the non-immersive interactive gaming platforms and social media sites these same companies already run. And we presented evidence that similar predatory behaviors are already being observed in the social media-modelled spaces within the metaverse, such as in Meta's Horizon Worlds.

How is this allowed to happen? Assessment of expected harms and routes to prevention or redress in the metaverse requires grappling with the "veil of scale," a concept that we originate in this Article to describe a fundamental characteristic of interactive digital platforms as they have come to be structured over the course of the past three decades. In sum, as social media platforms relentlessly pursue growth, the scale of the platform creates a veil, behind which bad actors can enjoy an ephemeral and anonymous digital persona.

For any of the harms detailed above, if the tortfeasor is knowable and has a stable offline presence, they can likely be held accountable. Our expectation is that for most of the "It didn't work in real life" harms detailed above, the parties upon whose reliance users depended will be established corporate actors, knowable and reachable through standard, direct tort action. The same will be true of some of the harms in the

category of virtual property disputes, when a transacting party is visible and reachable.[184]

In contrast, direct action becomes flatly unworkable when the tortfeasor is either (1) unknowable, having acted via an anonymous and ephemeral avatar or account; (2) judgment proof because they are located in a different jurisdiction; or (3) as routinely happens—both. The institutions and procedures of civil action or of criminal investigation and prosecution against harm-doers are not automatable and do not scale.[185] But opportunities for harm do scale. And they do so precisely because bad actors hide behind the "veil of scale."

Some sense of this imbalance is offered by one of the rare success stories of law enforcement action against a mass CSAM purveyor: the takedown of "Welcome to Video," a website based in South Korea that hosted and sold access to videos of child sexual abuse. More than 250,000 videos were found on the server, constituting "more content by volume than in any child sexual abuse materials case in history."[186] In 2018, a large

---

[184] However, we note the frequency with which supposedly large and established actors in, for instance, NFT issuance or cryptocurrency trading have turned out to be close to ephemeral themselves, with onetime assets disappearing in smoke to the chagrin of bankruptcy administrators. *See, e.g.*, Press Release, Sec. & Exch. Comm'n, *SEC Charges Samuel Bankman-Fried with Defrauding Investors in Crypto Asset Trading Platform FT* (Dec. 13, 2022) (According to the release "defendant concealed his diversion of FTX customers' funds to crypto trading firm Alameda Research while raising more than $1.8 billion from investors."), https://www.sec.gov/news/press-release/2022-219. In addition, there is a vast array of smaller and weirder cases. *See, e.g.*, Sarah Martin, *Chief Executive of Collapsed Crypto Fund HyperVerse Does Not Appear to Exist*, GUARDIAN (Jan 3. 2024) https://www.theguardian.com/technology/2024/jan/04/chief-executive-of-collapsed-crypto-fund-hyperverse-does-not-appear-to-exist.

[185] To read more about the role of the Fourth Amendment in disrupting the ability of criminal law enforcement to counter the "veil of scale," see discussion *infra* at Section III.A.

[186] Andy Greenberg, *Inside the Bitcoin Bust That Took Down the Web's Biggest Child Abuse Site*, WIRED (Apr. 7, 2022), https://www.wired.com/story/tracers-in-the-dark-welcome-to-video-crypto-anonymity-myth/; Press Release, Int'l Ctr. for Missing & Exploited Child., *Cryptocurrency and the Trade of Online Child Sexual Abuse Material* (Feb. 2021), https://www.icmec.org/press/new-report-examines-cryptocurrencys-role-in-online-child-sexual-exploitation/ [https://perma.cc/VH68-76FF].

international and interagency team managed to take the site down, seizing the server and arresting the man who ran it. The team sent detailed "targeting packages" to law enforcement agencies worldwide about the suspected perpetrators they were able to identify. By 2022, 377 arrests had been made, and 23 children removed from situations in which they were being actively exploited.[187]

In this case, there was a clear digital route to trace buyers and sellers, through barely-masked bitcoin transfers. There were well-developed institutional structures for international law enforcement collaboration. A dedicated team of uniquely skilled and obsessive pursuers happened to be available.[188] Their speed was impressive: the server was shut down in a matter of months and initial arrests of the highest priority perpetrators began immediately and continued for several years. Yet still, the hundreds of arrests represented only a fraction of the thousands of accounts that had existed on the site. The 250,000 videos interdicted seems like a large number, until one compares it to the 18 million reports of suspected CSAM to the NCMEC in the year of the takedown, 2018:[189] a total that would rise to over 31 million reports, including 49 million images and 38 million videos, in 2022 alone.[190] And of course, even these grim totals represent an unknowable fraction of the total CSAM imagery in circulation.

To reiterate, research suggests that twenty-nine percent of children aged 9-12 and forty-eight percent of children aged 13-17 in the United States—so, 4,726,351 9-12 year olds and

---

[187] *Id.*

[188] Greenberg, *supra* note 186.

[189] NAT'L CTR. FOR MISSING AND EXPLOITED CHILD., 2018 YEAR END REVIEW 5 (2018), https://www.missingkids.org/content/dam/missingkids/pdfs/2018%20Year%20in%20Review-web.pdf [https://perma.cc/GTQ7-45MP].

[190] NAT'L CTR. FOR MISSING AND EXPLOITED CHILD., CYBERTIPS 2022 REPORT (2022), https://www.missingkids.org/content/dam/missingkids/pdfs/2022-CyberTipline-Report.pdf [https://perma.cc/44YW-5AL4].

10,382,574 13-17 year olds[191]—have been pressured online to send sexual imagery to someone they only know online. Who are these perpetrators? How can they be brought to justice? The vast majority are in practice untouchable, shielded by the "veil of scale." And the same social media companies who generated these criminogenic circumstances in the non-immersive social media spaces that they run, are seeking to replicate their business model/monetization scheme in the metaverse.

*****

In this section we have outlined three very different types of harms: (1) problems that arise from "virtual showrooms" that promise things in the immersive environment that are a far cry from what is actually delivered; (2) disputes related to ownership rights, which will take very different courses depending on whether the counterparties are known actors or not; and (3) problems generated by largely unknowable predators who have taken advantage of the corporate engineered "veil of scale" that prioritizes exponential product growth—where the "product" is the user.

As different as these three categories of harms are, they do share a common trait: in each instance highlighted above, the interactions that lead to these harms are primarily personal, user-to-user interactions. This fact renders the statutory frameworks discussed in Part III below largely ill-suited to provide proper redress. In Part III, we elaborate on the inadequacy of each.

III. The Imperfect Intersection of Many Statutory Frameworks

When predictable harms, such as those discussed above, occur within rapidly evolving technological contexts, lawmakers have focused on either creating new statutes or re-

[191] Press Release, *U.S. Census Bureau, Growth in U.S. Population Shows Early Indication of Recovery Amid COVID-19 Pandemic* (Dec. 22, 2022), https://www.census.gov/newsroom/press-releases/2022/2022-population-estimates.html [https://perma.cc/P28F-SFXW]; U.S. CENSUS BUREAU, POPULATION PERCENTAGE BY AGE AND GENDER, (2022), https://www.census.gov/popclock/data_tables.php?component=pyramid [https://perma.cc/M4NJ-87DR].

tooling old ones to assist in making victims of these harms whole. Some of these statutory frameworks, such as data privacy laws, are used to provide protections and empowerments to users on an individual basis.[192] Others, such as antitrust laws, are used primarily to target the companies' actions, aiming to create "a level playing field" by limiting the power given to social media companies. However, as we argue below, many of these frameworks are limited by the subject matter and methodology of the laws. Even with some statutes that could conceivably be more useful—such as laws related to intellectual property ownership—they are useful only in cases where the perpetrator is known. When the perpetrators are ephemeral, these statutes have limited value.

Many of the statutes discussed were originally posited within other types of technology and data-driven harms. For instance, statutes that provide data privacy protections grew out of the development of big data and the subsequent commodification of user data necessitated by big data development. [193] However, given the current trajectory of corporate use of technology within the metaverse, these statutes will likely prove inadequate to address the harms that will unfold there.

In addition, while we focus primarily on *civil* action throughout this Article, many of the harms, particularly those related to child sexual exploitation, also have a criminal law counterpart. As such, we start with a brief deviation into criminal law and the Fourth Amendment, to spell out why current statutory models are unable to correct criminal harms masked by the "veil of scale." We do this to highlight the importance of our premise liability proposal in Section IV.B., which offers both a route to individual redress and a means to incentivize preventive action by platforms, under

---

[192] These tend to be done from a consumer protection paradigm. *See, e.g.*, discussion *infra* Section III.B, for the consumer paradigm at play in data privacy laws.

[193] *See* Jena Martin, *Data Privacy Issues in West Virginia and Beyond: An Overview*, at 6 (2nd Ed. Center for Consumer Law and Education White Paper 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4896449 [https://perma.cc/889K-CCU3].

circumstances in which law enforcement is systematically unable to address widespread criminality.

Then, we embark on a brief review of two of the most-discussed statutory proposals, data privacy statutes and antitrust laws, before concluding that these frameworks are, at best, a stop-gap to a long term solution or, at worst, potentially counterproductive to the aims of making victims of category 3 harms whole.[194] As such, the current statutory scheme does little to provide a comprehensive framework that would adequately address the myriad ways that users can negatively interact with others in the engineered environment of the metaverse.[195]

A. Criminal Law

Some acts effectuated via virtual interactions create clear real-world harm; we agree with other scholars who conclude these harmful acts should be criminalized. [196] However, the "veil of scale" (whose origins are delineated in Section I.B. and impact in Section II.D), when combined with the limitations embodied in the Fourth Amendment, gets in the way. As Prof. Kosseff explains:

> Before law enforcement can search the contents

---

[194] For instance, Section 230 of the CDA (which we discuss *infra* in Section IV.C) is not applicable to this analysis as it focuses on protections for platform owners. Here we are examining statutory frameworks that provide redress to harmed individuals.

[195] This is not a comprehensive list of every possible law; rather it is a general overview of the types of laws that have been discussed as routes to accountability or reform in this latest iteration of the Web. We also take this opportunity to note that this Article does not address many of the other constitutional implications that arise within this space. For instance, while some have discussed many of the experiences within a free-speech paradigm, we believe that the nature of the interaction does not easily lend itself to this analysis. *See* Cyphert & Martin, *supra* note 9; *see also* Danielle Keats Citron & Mary Anne Franks, *The Internet as a Speech Machine and Other Myths Confounding Section 230 Speech Reform*, 2020 U. CHI. L. F. 45 (2020).

[196] Clarke, *supra* note 168; Kerr, *supra* note 3 at 415; Balkin, *supra* note 3, at 2045; Hunter & Lastowka, *supra* note 3, at 294 (asking if "non-consensual appropriation and destruction of virtual properties . . . might be seen as truly criminal").

> of emails, chat logs, and other private communications, the Fourth Amendment generally requires that they obtain a warrant supported by probable cause. What about the private companies that provide the services? Can't they automatically or manually search their users' private accounts for evidence of a crime and then share that information with the government? The answer to that question, from a Fourth Amendment perspective, is not always easy, and it points to one of the most substantial barriers to public-private partnerships in investigating distributors of child sex abuse material and other illegal content.[197]

Specifically, while the Fourth Amendment does not prevent private actors from accessing users' data, if the private actor is doing so with at least some approval, support, or acquiescence by law enforcement, the line between private party and government actor becomes murky indeed. So, while a private party's search results proactively turned over to a government official would not be grounds for a Fourth Amendment bar under the exclusionary rule, if that same government actor expands upon the search, the subsequently found evidence will almost assuredly have been obtained in violation of constitutional protections.[198]

At the same time, the "veil of scale" makes typical law enforcement protocols unworkable for many online harms. For instance, the idea of law enforcement seeking warrants for each suspected perpetrator individually becomes unworkable when perpetrators number in the thousands, are dispersed worldwide, and hide behind ephemeral and anonymous accounts. Contemplating how this would work in practice helps us see exactly how scale is crucial to creation of the "veil of scale." Hackers who steal images worth thousands of actual dollars in Roblox credits, for example, commit a clear-cut

---

[197] Jeff Kosseff, *Private Computer Searches and the Fourth Amendment*, 14 I/S: J. L. & Pol. 187 (July 1, 2018), https://ssrn.com/abstract=3225742 at 2.
[198] *Id.*

crime, one that is allegedly quite common. But what form could a law enforcement crackdown against this crime wave take? Do we expect law enforcement agents to accumulate enough evidence from publicly visible sources about individual avatars to convince judges to issue warrants against, for instance, "a beamer called Max" or the account "1nsider"?[199]

It is far more practicable to rely on platforms, rather than individual perpetrators, to make changes to deter crimes and provide partial redress.[200] However, without stronger incentives for platforms to take on this role proactively, accountability will likely languish.[201] This is the clear message from the slew of whistleblower action by current and former Meta employees in recent years, who attest to decision after decision taken to prioritize growth and engagement over the reduction of risk and harm.[202]

As such, using criminal law to mitigate harms that will occur within the metaverse is unlikely to yield significant results vis-à-vis harms in the social media and interactive gaming-modelled metaverse, where the "veil of scale" will

---

[199] Cox, *supra* note 124. For an early discussion of how the federal Computer Fraud and Abuse Act, on the one hand, and the common law of trespass to chattels, on the other, apply to disruption of access in virtual digital environments, see Smyth, *supra* note 3.

[200] This indeed seems to have partially happened in the Roblox case discussed above. *See* Cox, *supra* note 124. *See also* @SkilledSniper1, ROBLOX DEV. F. (May 2021), https://devforum.roblox.com/t/how-to-prevent-and-react-to-stolen-models/1216873 [https://perma.cc/M793-4CBY].

[201] One might think consumer choice would be incentive enough because users have the option to simply walk away to competitors' offerings if they are exposed to harassment or crimes on one platform. However, as detailed above, network effects function to create concentration in the social media sector. In theory, even within a duopoly, platforms might compete by offering higher standards of user safety. In practice, the market has never seen this happen, possibly because competing firms share an interest in keeping opaque the incidence of harm to users on their platforms.

[202] *See* HORWITZ, *supra* note 102; Justin Hendrix, *Transcript: Senate Hearing on Social Media and Teen Mental Health with Former Facebook Engineer Arturo Bejar*, TECH POL. PRESS (Nov. 8, 2023), https://www.techpolicy.press/transcript-senate-hearing-on-social-media-and-teen-mental-health-with-former-facebook-engineer-arturo-bejar/ [https://perma.cc/6EZR-DHAR].

prevail. In the Sections that follow, we assess whether civil statutes might fill the gap.

B. Data Privacy

Scholars have long discussed the evolution of data privacy issues in tandem with the scale of technology. As one of us noted in a previous work:

> One of the biggest changes that impacted privacy in the last few decades has been businesses' ability to collect, keep and utilize data digitally. . . . Now, in theory, there are few limits to the amount of information that a business can acquire about you – leading some leading scholars to proclaim that many businesses know more about you then you know about yourself.[203]

This will likely continue within the metaverse. As current practitioners note:

> [P]latforms could (as they do now) collect data about what users buy in the metaverse, what they look at, and their conversations with other users. However, because a user's access to the metaverse would be through a headset, much more data could be collected – for example, relating to user movements, physiological responses, and perhaps even brainwaves – that will give platforms a deeper understanding of their users' thought patterns and behaviors.[204]

To address these concerns, lawmakers have sought to offer some protection. Beginning in Europe in 2016 and then following in some states within the United States, legislators have passed laws that encompass a wide range of protections for consumers, including allowing them to opt out of any collection methods that a corporation might use or requiring their permission to collect data when they are surfing the

---

[203] Martin, *supra* note 193.
[204] DiMatteo & Russell, *supra* note 147.

internet.[205]

However, the locus of harm that these statutes are addressing is misaligned with the nature of the interactions with which this Article is generally concerned. For instance, as discussed in Part II, the most significant harms that will come in the metaverse will be as a result of *forward-facing*, one-on-one user interactions (either between a user and a corporation or between a user and an ephemeral bad actor). In contrast, the harms that data privacy statutes are trying to address are largely related to "back of the house" operations—that is, those instances where a user's *data* (rather than the user themself) is interacting with another in a way that produces harm.

In addition, many of the harms that comes from a lack of data privacy happen in a diffuse, cumulative manner. Intrusive data gathering happens at the device level, aggregating data across online interactions.[206] But it is not the customer's own data that produces the harm on its own. Rather, it is what the corporation can extrapolate from that data—along with the data it has extracted from *millions* of other users—that truly exacerbates the problem for the user. In that regard, minimizing the amount of data that a corporation can use, as most data privacy laws do, is an appropriate remedy. In contrast, the harms that we discuss in Section II.B are devastating to individual users via individual interactions. Platform-facilitated criminogenic access, rather than platform data accretion, is the driver.

It is true that real action on data privacy could destabilize the data-exhaust-driven business model of social media platforms, and in turn change the dynamics that produce the

---

[205] *See generally* Martin, *supra* note 193 (providing an overview of date privacy laws as of 2024).

[206] Fran Mariutti, *New Study Reveals the Most Invasive Apps Collecting Your Data*, NATIONALWORLD (Sept. 5, 2024), https://www.nationalworld.com/lifestyle/tech/new-study-reveals-the-most-invasive-apps-collecting-your-data-4769675; Stuart A. Thompson & Charlie Warzel, *Smartphones Are Spies. Here's Whom They Report To*, N.Y. TIMES (Dec. 20, 2019), https://www.nytimes.com/interactive/2019/12/20/opinion/location-tracking-smartphone-marketing.html.

"veil of scale." However, so far, dominant platforms have often been able to adapt to new privacy regulations with the equivalent of adding a few more clicks to the process of account creation or website access, with little effect on the "veil of scale."[207]

Finally, data privacy statues could indeed offer some protection for consumers whose information is being tracked by corporations when they interact with the corporation's IR technology.[208] Yet, in other ways, data privacy laws could be used in a much more deleterious manner. Specifically, the foundational structure of these laws allows users the right to opt out of collection methods for some of their interactions.[209] This, in turn, risks exacerbating the problems that occur in one-on-one interactions with ephemeral predators: platforms can allege that the need to preserve users' privacy hampers their ability to flag serial violators across multiple accounts.[210] And clearly, there are real trade-offs between maximizing privacy protection and maximizing platform oversight of vulnerable

---

[207] Shoshana Wodinsky, *The Hidden Failure of the World's Biggest Privacy Law*
The EU's landmark privacy law, GDPR, was supposed to change the world of tech privacy forever. What the hell happened? GIZMODO (Feb. 4, 2022), https://gizmodo.com/gdpr-iab-europe-privacy-consent-ad-tech-online-advertis-1848469604 [https://perma.cc/J4AF-KPNY].

[208] Luis Quintero, *A New Wave of Wearable Devices Will Collect a Mountain on Information on Us—We Need to Get Wise About the Privacy Implications*, THE CONVERSATION (Apr. 17, 2024), https://theconversation.com/a-new-wave-of-wearable-devices-will-collect-a-mountain-on-information-on-us-we-need-to-get-wise-about-the-privacy-implications-226537 [https://perma.cc/SN8W-7YTD].

[209] *See, e.g.*, Cal. Code, Cal. Civ. Code § 1798.100 (California Data Privacy Act) (providing key protections for consumers by limiting what data a corporation can collect). Like anything, data privacy laws are tools—they can sometimes help and sometimes hurt depending on the circumstances. For a discussion of ways in which data privacy laws benefit consumers, see Jena Martin, *Data Privacy Issues in West Virginia: An Overview*, 124 W. VA. L. REV. ONLINE 1 (2021). For a discussion of several data privacy laws across the country, see Martin, *supra* note 193.

[210] *See* Jess Weatherbed, *Roblox, Discord, OpenAI, and Google found new child safety group,* THE VERGE (Feb. 10, 2025), https://www.theverge.com/news/609367/roblox-discord-openai-google-roost-online-safety-tools [https://perma.cc/2JJ2-UFAV].

users: this trade-off has been at the fore in recent debates over end-to-end encryption on the one hand and proposed age-verification requirements on the other.[211]

In sum, pro-forma pro-privacy measures may just provide an alibi for platforms' failure to trace and act against actors committing harms, while not bringing about more fundamental change.

C. Antitrust

Increasingly, regulators have been turning to antitrust laws to help tame the behavior of technology corporations. Lawsuits against Amazon, Google, and others have been filed with increased regularity in recent years.[212] Meta, while not completely immune, is likely currently inoculated from these attacks. In April 2023, in what commentators called "a sweeping victory" for the tech giant, the U.S. Court of Appeals for the D.C. Circuit upheld a federal district court's dismissal of a lawsuit filed by twenty-seven state regulators. The complaint argued that Meta created a "monopoly power in the personal social networking market in the United States [and] illegally maintains that monopoly power by deploying a buy-or-bury strategy that thwarts competition and harms both users and advertisers. Strategies for engaging children across multiple platforms involved deceptive acts and unfair methods of competition."[213] The district court, in dismissing the complaint, did not reach the merits of the claims, but rather stated that the allegations were barred by the statute of

---

[211] *See* Electronic Frontier Found., Comment Letter (Sep. 30, 2024) https://www.eff.org/document/eff-comments-ny-ag-safe-kids-sept-2024 [https://perma.cc/4VBH-4YVD].

[212] *See* Diego Lasarte, *The Ongoing Big Tech Antitrust Cases to Watch in 2023*, QUARTZ (Jan. 24, 2023), https://qz.com/antitrust-cases-big-tech-2023-guide-1849995493.

[213] Compl. at ¶ 4, State of New York v. Facebook, No. 1:20-cv-03589-JEB (D.D.C. Dec. 9, 2020).

limitations.[214] The D.C. Circuit affirmed on similar grounds.[215]

Meanwhile, law makers have been attempting, specifically, to re-engineer current antitrust laws to explicitly target tech companies. For instance, in the 2021 congressional session, at least five bills were introduced with the aim of targeting the monopolies built by tech companies.[216]

Antitrust theories are also being used successfully by the federal government. For instance, on August 5, 2024, in what has been called the "biggest tech monopoly trial of the 21st century," [217] between the Department of Justice (DOJ) and Google, Judge Amit Mehta of the U.S. District Court for the District of Columbia ruled that Google had violated antitrust laws by creating "an illegal monopoly [to] become the

---

[214] Brian Fung, *Federal Appeals Court Tosses State Antitrust Suit Seeking to Break Up Meta*, CNN (Apr. 27, 2023), https://www.cnn.com/2023/04/27/tech/meta-federal-appeals-court-antitrust-suit/index.html#:~:text=A%20group%20of%20states%20that,victory%20for%20the%20tech%20giant [https://perma.cc/AB27-M4P6]. State Attorneys General, undeterred, filed another lawsuit against the tech giant, claiming that its two most prominent platforms, Facebook and Instagram, were addicting to children. Compl. State of Arizona et al. v. Meta Platforms, Inc. et. al, Case 4:23-cv-05448-YGR (Nov. 22, 2023). *See also* discussion *infra* Section IV.A.

[215] *Id.* The idea of using antitrust laws in litigation against tech companies was first raised by a law student named Lina Khan. *See* Lina Khan, Note, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710 (2017). The idea turned into action after Sen. Elizabeth Warren (herself a former law professor at Harvard) met with Khan and discussed the contours of a strategy. *See* Sheelah Kolhatkar, *How Elizabeth Warren Came Up with a Plan to Break Up Big Tech*, THE NEW YORKER (Aug. 20, 2019), https://www.newyorker.com/business/currency/how-elizabeth-warren-came-up-with-a-plan-to-break-up-big-tech [https://perma.cc/H5FP-RE9G].

[216] Cecilia Kang, *Lawmakers, Taking Aim at Big Tech, Push Sweeping Overhaul of Antitrust*, N.Y. TIMES (June 29, 2021), https://www.nytimes.com/2021/06/11/technology/big-tech-antitrust-bills.html.

[217] *See* Dara Kerr, *United States takes on Google in biggest tech monopoly trial of 21st century*, NPR (Sept. 12, 2023), https://www.npr.org/2023/09/12/1198558372/doj-google-monopoly-antitrust-trial-search-engine#:~:text=The%20Justice%20Department's%20case%20hinges,was%20to%20stomp%20out%20competition [https://perma.cc/6FXC-2TWD].

world's largest default search engine."[218] The government claimed that Google has used business dealings and other illegal tactics to create a stranglehold on the internet that amounts to an illegal monopoly.[219] The move marked the first time that the DOJ attempted to use an antitrust framework against one of the Big Tech firms. Given the judge's ruling in favor of the DOJ's theory, it is likely not the last.

While there is definite value to examining the antitrust dimensions of tech firms and the internet generally, we do not think that the antitrust laws as they are currently conceived offer much help toward limiting individual-level harm in the metaverse. Just as with data privacy laws, the challenges that antitrust laws are designed to prevent are quite distinct from the cauldron of harms presented by user-to-user interactions. The "veil of scale" that we have pointed to in this Article is generated by the free-and-frictionless-account-formation strategy adopted by social media platforms in pursuit of scale, but its functioning is not directly dependent on the scale of individual platforms, nor on the scale of the corporations that own them. Any social media or interactive gaming platform seeking growth through the proliferation of ephemeral and externally untraceable accounts generates the same basic dilemmas. Moreover, bad actors already move interactions with child victims across platforms, taking advantage of the distinctive affordances of each.[220]

To be sure, platforms with especially massive user bases such as Facebook and Roblox provide particularly attractive attack surfaces for bad actors. Yet while breaking up those platforms might slightly slow the algorithmically accelerated pursuit of victims, it would also multiply the number of corporate entities that victims and law enforcement might need

---

[218] David Shepardson and Mike Scarcello, *Google Has an Illegal Monopoly on Search, U.S. Judge Finds*, REUTERS (Aug. 5, 2024), https://www.reuters.com/legal/us-judge-rules-google-broke-antitrust-law-search-case-2024-08-05/.

[219] Kerr, *supra* note 217.

[220] David Thiel, Renée DiResta and Alex Stamos, *Cross-Platform Dynamics of Self-Generated CSAM*, STAN. INTERNET OBSERVATORY (June 7, 2023), https://stacks.stanford.edu/file/druid:jd797tp7663/20230606-sio-sg-csam-report.pdf.

to interact with. In other words, fragmenting the veil of scale would not make it more penetrable. Indeed, as one of us wrote previously, just as with data privacy laws, the use of antitrust statutes in this instance could have harmful effects.

> Although there may be reasons to be more skeptical about mergers and to have better laws in place to prevent monopolistic behavior, simply "breaking up" a company like Facebook is unlikely to solve the problems that arise, . . . a point that whistleblower Frances Haugen made in her October 2021 testimony before Congress. . . . Haugen testified that breaking up Facebook would not remove the dangerous algorithmic amplification that occurs on the site but would remove some of the content moderation resources.[221]

In sum, current statutory frameworks and criminal law enforcement are largely incapable of addressing the magnitude of harm at stake. As we noted above, this provides platforms with little incentive to address the issue. At a minimum, we believe that existing statutes should be robustly supported by individual civil actions (or even class action litigation) as a way to provide both accountability for those who play a role in perpetuating the harm and as a way of providing remediation for those who have suffered.

Could a premise liability framework provide the needed incentive?

IV. The Heart of the Matter – Using an Old Legal Model Within a Decidedly New Environment

> *As a general rule, a private person does not have a duty to protect another from a criminal attack by a third person. . . . But the rationale of this very broad general rule falters when it is applied to the conditions of modern-*

[221] Cyphert & Martin, *supra* note 9 at 170.

> *day urban apartment living. . . . In the case at bar we place the duty of taking protective measures guarding the entire premises and the areas peculiarly under the landlord's control against the perpetration of criminal acts upon the landlord, the party to the lease contract who has the effective capacity to perform these necessary acts.*[222]

Who is responsible for preventing third-party harm in this new kind of shared space? That was the question presented to the D.C. Circuit Court in 1970, after Sarah Kline was assaulted in the common hallway of her apartment building whose owners had failed to take basic preventive measures (locks, guards, doormen) despite an accelerating series of crimes carried out by intruders in the building's common spaces. The trial court had relied on the traditional common law distinction between a landlord's minimal role and an innkeeper's duty of care to protect guests from third-party harm on the premises, but the circuit court ruled that modern living arrangements had evolved to a point where a landlord's role encompassed this duty as well. Specifically, the court found that the landlord "is the only one who is in a position to take the necessary protective measures for overall protection of the premises, which he owns in whole and rents in part to individual tenants."[223]

As we have argued above, the unique dilemma presented by the social media/interactive gaming metaverse is the prevalence of torts and crimes committed within the virtual setting by third parties who are untouchable by external law enforcement or civil remedy. Unique among tort categories, premises liability has a carefully developed jurisprudence regarding the nature and extent of liability for third-party harms. Moreover, as we see with the courts' changing jurisprudence after the 1970 *Kline v. Mass. Ave.* decision, this is a realm where it is understood that, as the way we live our

---

[222] Kline v. 1500 Massachusetts Ave. Apartment Corp., 439 F.2d 477 (D.C. Cir. 1970).
[223] *Id.*

lives evolves—and as the risks we face evolve, and the practicalities of *who* can take steps to mitigate those risks evolves—the allocation of legal responsibility must evolve as well.

To that end, this Part first plots the distinct theories of tort law that can support the application of premises liability to the social-media-modelled metaverse. Second, we look at three specific components of premises liability tradition that are particularly well suited to application vis-à-vis platform-engineered virtual space. Third, we review some additional tort claims that have been recently applied to social media harms, showing that these are complementary to, but do not take the place of, premises liability. Finally, we argue that assessing premises liability in the metaverse need not run afoul of Section 230's injunction on the treatment of interactive computer services as publishers of other parties' speech.

A. Just Recompense and Economic Efficiency: Two Theories of Tort Liability in Virtual Social Space

The foundational notions of criminal justice have long been said to (1) vindicate societal harms; (2) deter future crimes and (3) punish and remove bad actors from society.[224] In turn, private tort litigation is undergirded by two reinforcing notions: (1) law enforcement is inadequate, on its own, to address every harm that occurs within society and, as such, (2) tort law serves as a complementary structure for legal harms.[225]

On its face, tort law's status as a parallel counterpart to criminal law is suited to the social media and interactive gaming metaverse. As detailed above, virtual interactions can lead to

---

[224] For a discussion of the first two principles, see Paul Robinson, *A Functional Analysis of Criminal Law*, 88 N.W. REV. 357 (1994). For a discussion of the third, see Alex Raskolnikov, *Criminal Deterrence: A Review of the Missing Literature*, 28 SUP. CT. ECON. R. 1 (2020).

[225] For a general discussion of how private litigation can supplement enforcement actions in the United States, *see* J. Maria Glover, *The Structural Role of Private Enforcement Mechanisms in Public Law*, 53 WM. & MARY L. REV. 1137 (2012). For an example of how that looks in specific fields (in this case, the securities industry), *see* J.I. Case Co. v. Borak, 377 U.S. 426 (1964), which states that "private enforcement of the proxy rules provides a necessary supplement to Commission action."

concrete real-world harms, in some cases clearly matching criminal acts. Yet because of the systemic characteristics of platform architecture and monetization strategy—to wit, the veil of scale these together create—these crimes cannot effectively be policed.

To that end, a premise liability cause of action can be justified under both (1) a retributive theory and (2) an economic efficiency argument. We first address the justice or retributive theories of torts, which foreground the importance of rights, wrongs, and redress.[226] As scholar Richard Wright spells out,

> people generally believe that it is not properly respectful of the equal dignity and autonomy of others, and hence not just, for you to create substantial unaccepted foreseeable risks of injury to others' persons or property merely for your own personal benefit, even if your expected gain will exceed their expected loss. Indeed, corporations and individuals who are thought to have done so are often held liable for punitive damages.[227]

The intuitive application vis-à-vis the platforms building the social-media-modelled metaverse is clear. The social media corporations replicating their mass monetization model in the metaverse have profited enormously from its prior implementation in non-immersive social media platforms, while opening the door for unprecedented kinds of harm, like sexual exploitation of children by unattainable criminals who never leave their homes halfway around the world from the victims. The moral intuition that it is unjust for Meta and similar platforms to reap multimillion dollar profits from a business that sells users' private data, has a negative impact on

---

[226] For a comprehensive discussion of other theoretical constructs of tort law, including the support of community, see Cristina Carmody Tilley, *Tort Law Inside Out*, 126 YALE L.J. 1320 (2017).

[227] Richard W. Wright, *Hand, Posner, and the Myth of the "Hand Formula,"* 4 THEO. INQ. L.J. 145, 147 (2003).

society,[228] and creates criminogenic spaces where children get hurt[229] is widely shared. And the speed with which social platform Omegle settled as soon as a lawsuit over online sexual abuse survived a motion to dismiss under Section 230 may suggest their recognition of just how eager juries might be to award massive monetary damages to individual children as recompense for the intense harm experienced in their virtual space.[230]

The second approach to torts emphasizes aggregate economic efficiency instead, focusing less on the need to compensate harmed individuals per se than on the instrumentalist rationale that tort law serves the social good by incentivizing efficient resource allocation.[231] Under this theory, it is important to identify the "cheapest-cost-avoider" and ensure (via legal liability) that they shoulder the cost of allowing harms to happen. This properly incentivizes investment in deterrence by the actor most efficiently placed to achieve it.[232]

Given that social media platforms (both non-immersive and within the metaverse) invite users in as the core of their business model, and have a knowledge of and ability to control their space that none of the invitees has, the relationship is best

---

[228] *See, e.g.*, Heather Kelly & Emily Guskin, *Americans Widely Distrust Facebook, TikTok and Instagram with Their Data, Poll Finds*, WASH. POST (Dec. 22, 2021), https://www.washingtonpost.com/technology/2021/12/22/tech-trust-survey/.

[229] Cory Combs, *New Poll Finds Overwhelming Public Support for Bipartisan Legislation to Protect Kids From Online Harms*, ISSUE ONE (Nov. 16, 2023), https://issueone.org/press/new-poll-finds-overwhelming-public-support-for-bipartisan-legislation-to-protect-kids-from-online-harms/#:~:text=Nearly%20all%20voters%20(94%25),over%20the%20last%2020%20years [https://perma.cc/4Z3A-UQXD].

[230] Bill Chappell, *Video Chat Site Omegle Shuts Down After 14 years — And an Abuse Victim's Lawsuit*, NPR (Nov. 9, 2023, 5:01 PM ET), https://www.npr.org/2023/11/09/1211807851/omegle-shut-down-leif-k-brooks [https://perma.cc/Z4EW-2VZV].

[231] Richard A. Posner & William M. Landes, *The Positive Economic Theory of Tort Law*, 15 GA. L.R. 851 (1980).

[232] WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW 92-95 (1987).

analogized to the special relationship of innkeeper to guest.[233] Here, the reasoning of *Kline v. Massachusetts Avenue*, in extending innkeepers' traditional duty to seek to prevent third-party harms to the landlords of modern multi-unit dwellings, is particularly apt. Indeed, the court in *Kline* detailed the circumstances that make the landlord the least-cost-avoider in such a setting, where it is essential to incentivize landlords to take proactive steps in order to achieve societally optimal levels of deterrence:

> Not only as between landlord and tenant is the landlord best equipped to guard against the predictable risk of intruders, but even as between landlord and the police power of government, the landlord is in the best position to take the necessary protective measures. Municipal police cannot patrol the entryways and the hallways, the garages and the basements of private multiple unit apartment dwellings. They are neither equipped, manned, nor empowered to do so. In the area of the predictable risk which materialized in this case, only the landlord could have taken measures which might have prevented the injuries suffered by appellant.[234]

Application of this reasoning to the social metaverse is clear. Because the companies building and running social metaverse platforms have unique capacity to observe and mitigate risks, they are the least-cost-avoiders who should bear the cost of avoidable harms they fail to prevent. If they are shielded from those costs, the overall investment in safety will be suboptimal, inefficient, or both.[235]

Finally, it is worth noting that the case for tort liability

---

[233] For a discussion of special relationships and how they have been held to impact premise owners' liability for third party harm, *see* Walls v. Oxford Management Co., 137 N.H. 653 (1993).

[234] Kline v. 1500 Massachusetts Ave., 439 F.2d 477 (D.C. Cir. 1970).

[235] For a detailed development of this line of reasoning, see Geoffrey A. Manne, Kristian Stout & Ben Sperry, *Who Moderates the Moderators?: A Law & Economics Approach to Holding Online Platforms Accountable Without Destroying the Internet*, 49 RUTGERS COMPUTER TECH. J. 1 (2021).

within the metaverse aligns with economic efficiency analyses of when tort action, rather than regulation, will be optimally rational. Shavell's classic assessment points first and foremost to cases in which regulatory authorities have radically less knowledge about risks underway than the parties creating those risk.[236] Given the pace and complexity of technological change shaping interactive virtual space, and the lack of external visibility into patterns of harm as shaped by continually shifting algorithmic implementations,[237] regulatory mandates will be predictably cumbersome at best, and counterproductive at worst.[238] A tort regime geared to balance costs against risk reduction—as the premises liability tradition explicitly does—will create better-calibrated, results-focused incentives.

Clearly, some jurists are sympathetic to this need. Novel tort theories such as products liability are currently seeing some success in litigation against social media companies, while also generating reversals and circuit splits.[239] We will discuss

---

[236] Steven Shavell, *Liability for Harm versus Regulation of Safety*, 13 J. LEGAL STUD. 357 (1984).

[237] *See generally* HORWITZ, *supra* note 102 (describing a plethora of examples of highly impactful algorithmic shifts within Meta's social media platforms that were only revealed years later by whistleblowers' leaks).

[238] For instance, we note the sobering fact that even legislative action on a clear and bipartisan goal—reducing the use of the internet for sex trafficking, especially of minors—resulted in internally contradictory legislation that has brought counterproductive results. Eric Goldman, *The Complicated Story of FOSTA and Section 230,* 17 FIRST AMEND. L. REV.279 (2019; Danielle Citron & Quinta Jurecic, *FOSTA's Mess*, 26 VA. J. L. & TECH., 1 (2023).

[239] *See, e.g.* Daniel v. Armslist, LLC, 2019 WI 47, 926 N.W.2d 710 (Wis. A2019) (reinstating the dismissal of the case on Section 230 grounds); Peter Karalis & Golriz Chrostowski, *Product Claims Spike as SCOTUS Ponders Section 230 Fix*, BLOOMBERG L. (Mar. 2, 2023), https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-product-claims-spike-as-scotus-ponders-section-230-fix; Kevin Ofchus, *Cracking the Shield: CDA Section 230, Algorithms, and Product Liability*, 46 U. ARK. LITTLE ROCK L. REV. 27 (2023); Tyler Lisea, *Lemmon Leads The Way To Algorithm Liability: Navigating The Internet Immunity Labyrinth*, 50 PEPP. L. REV. 785 (2023). For further commentary on *Daniel v. Armslist*, see Eric

below some of these tort theories (products liability and public nuisance) recently essayed in litigation against non-immersive social media platforms, which may also find future application in litigation in response to metaverse harms. But we begin with the tort theory best suited for addressing the prevalence of third-party harms in (virtual) spaces that only owners/operators can effectively police: premises liability.

B. Specific Components of Premises Liability Offer a Particularly Useful Model for Third-Party Harms Shaped by Engineered Space

Common-law premises liability reflects, at its core, a basic moral intuition: owners or possessors owe a duty of care to people who enter into spaces they own or control. The required elements to establish liability are:

- The defendant owned or controlled the premises.
- The defendant failed to exercise "ordinary care" that would have prevented the harm, to wit:
  - The property owner knew or should have known about the hazard.
  - The property owner neither fixed the danger nor warned guests of the risk.
- The danger resulted in a severe, direct, and predictable injury.[240]

From this basic framework, premises liability jurisprudence has developed to encompass a wide array of types, circumstances, and sequences of injury, ranging from twisted ankles on broken or poorly designed stairways,[241] to tragic

---

Goldman, *Wisconsin Supreme Court Fixes a Bad Section 230 Opinion*, TECH. & MKT'G L. BLOG (May 7, 2019), https://blog.ericgoldman.org/archives/2019/05/wisconsin-supreme-court-fixes-a-bad-section-230-opinion-daniel-v-armslist.htm.

[240] RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL & EMOTIONAL HARM § 51 cmt. b, illus. 1, cmt. h, illus. 2-4, cmt. i, illus 5, cmt. j, illus. 6-7, cmt. u, illus. 8-13 (Tentative Draft No. 6, 2009); Stephen D. Sugarman, *Land-possessor Liability in the Restatement (Third) of Torts: Too Much and Too Little*, 44 WAKE FOREST L. REV. 1079.

[241] Murphy v. 210 Burwell Avenue, LLC, 2018 WL 1041499 (Conn. Super. Ct. Dec. 7, 2017).

drownings of children in unguarded swimming pools,[242] to renters who become victims of sexual assault when property owners fail to maintain adequate security.[243] While common law traditionally held that premises owners' duty of care depended on the circumstances of the injured party's presence on the property (trespasser, licensee, or invitee), these distinctions became somewhat less rigid in the wake of *Rowland v. Christian* (1968),[244] with the court insisting that even unlawful trespassers merit some duty of care from premise owners. Meanwhile the tradition has been staunch in treating child trespassers as distinct from adult trespassers, recognizing that children may routinely cross into premises to which they were not invited, especially if there are foreseeably attractive elements and no effective barriers to their entry.[245]

---

[242] Bennett v. Stanley, 92 748 N.E.2d 41, 43 35 (Ohio 2001); *see also* Mart v. Shea, 463 N.E.2d 1092, 1094 (Ind. 1984) (finding third-party horseplay precipitated the fall into the pool).

[243] *See, e.g.*, Veazey v. Elmwood Plantation Associates, Inc., 650 So. 2d 712 *discussed in* JONATHAN L. ZITTRAIN AND JORDI WEINSTOCK, TORTS! 20.4, (3d ed. 2022), https://opencasebook.org/author/zittrain/torts/.

[244] Rowland v. Christian, 443 P.2d 561 (Cal. 1968). Specifically, in the wake of *Rowland*, many jurisdictions explicitly followed the California Supreme Court's collapse of the distinctions *see*, *e.g.*, American Law Reports 4th, Modern Status of Rules Conditioning Landowner's Liability Upon Status of Injured Party (stating that, in the wake of *Rowland*, "a number of American jurisdictions have squarely approved the total rejection of the common law status classifications as determinative of liability" and citing cases in Colorado, D.C., Hawaii, Illinois, Louisiana, New Hampshire, New York, and Rhode Island). Ironically, the case that started this trend, *Rowland*, has itself been superseded by statute. *See* Calvillo-silva v. Home Grocery, 968 P.2d 65, 71-73 (Cal. 1998) (interpreting a California law enacted after *Rowland* to undo *Rowland*'s collapse of the distinctions). Importantly, we do not make a distinction here regarding what type of "presence" the current ephemeral tortfeasor is triggering, rather we leave to future works an analysis and application of those distinctions. However, we remain confident that regardless of what category of care is triggered, a strong case can be made for holding social media companies liable under a premises liability theory.

[245] *See Duty of Reasonable Care To Third Persons On The Premises*, 26 WASH. & LEE L. REV. 128 (1969); Carl E. Edwards Jr. Richard J. Jerome, *Torts - Negligence - Premises Liability: The Foreseeable Emergence of the*

We turn next to analyze specific components of premises liability jurisprudence that are well aligned with the complexities of risk, harm, and prevention in the social metaverse. This alignment is not happenstance, nor the fruit of a fishing expedition for a legal theory that might favor plaintiffs. Rather, these points of alignment result from the underlying organic connection: engineered spaces where members of the public enter and interact generate characteristic patterns of risk and associated dilemmas of responsibility. These patterns and dilemmas are highly analogous between physical and virtual spaces.

1. Third-Party Harm

As noted at the start of this Part, a well-established principle within premises liability is that under certain, but limited circumstances, premises owners can be held liable for predictable third-party harms. Successful cases include not only lawsuits against apartment complexes[246] but commercial locales, including grocery stores[247] that maintained poorly lit and unsurveilled parking lots where assaults occurred. In these specific cases, both the facts of frequent similar robberies in the area[248] and that basic industry standard preventive measures like better lighting and security cameras were not provided

Community Standard, 51 DENVER L. REV. 145 (1974); Robert S. Driscoll, *The Law of Premises Liability in America: Its Past, Present, and Some Considerations for Its Future*, 82 NOTRE DAME L. REV. 881 (2006).

[246] Nixon v. Mr. Property Management Co., 690 S.W.2d 546 (Tex. 1985).

[247] Clohesy v. Food Circus Supermkts, 293 N.J. Super. 217 (1996).

[248] *See e.g.*, Timberwalk Apts. Partners, Inc. v. Cain, 972 S.W.2d 749, 756 (Tex. 1998) (holding that "foreseeability is established through evidence of specific previous crimes on or near the premises"); *but see also* Nixon v. Mr. Property Management Co., Inc. 690 S.W.2d 546 (Tex. 1985) (holding that evidence of previous sexual assaults was not necessary to create a fact issue on foreseeability and that a history of other violent crimes in the area was sufficient); *Clohesy*, 293 N.J. 217 (stating that the court would no longer require "prior similar criminal incidents" on the defendant's premises to impose a duty on the defendant business owner, instead adopting a balancing test).

were weighed in evaluating liability.[249] Indeed, these two examples highlight the two main ways that duty of care analyses have been undertaken within the context of premises liability. Specifically, one strain of cases has analyzed the premise owners' duty of care relating to the condition of the premises.[250] Another strain of cases examines the premise owners' duty of care related to negligence in the conduct of activities on the premises.[251]

More fundamentally, when the New Hampshire Supreme Court in 1993 surveyed the circumstances under which courts have found that the standard presumption that actors are not responsible for preventing the crimes of others should be overridden to find a duty to act to prevent third-party harms, they found four exceptions, the first two of which are particularly relevant to the cases for premises liability in virtual space.

"The first arises when a special relationship, such as that of innkeeper-guest, or common carrier-passenger, exists between the parties"[252]—and, the 1993 court noted, since *Kline v. 1500 Massachusetts Avenue* jurists have followed the *Kline* court's conclusion that the modern landlord-tenant relationship is now analogous to that of innkeeper-guest. As we argued at the start of this Section, this evolution offers a useful precedent for extending the same logic now into virtual spaces. After all, as we have underlined throughout this Article, the entire business of Meta, Roblox, and their peers depends on inviting users in. Users are not only invited in *by* the platform owners, but for the platform owners' own benefit, since it is the users' presence that platform companies monetize to generate

---

[249] Andrew K. Miller, *Understanding Premises Liability for Third Party Crimes*, 80 ILL. B.J. 311 (1992); Bruce A. Jacobs, *Foreseeability and Duty of Care in Third-Party Premises Liability*, 35 BRIEF 54 (2006).

[250] *See* ALR, *supra* note 244.

[251] *Id.* We make no specific intervention in this Article regarding which duty of care analogy is best suited to application in the metaverse; indeed we find that there are enough similarities present in each strain of the cases that can be suitably applied. As such, we leave to future works a comprehensive unpacking of these distinctions as they would manifest in the world of immersive reality.

[252] Walls v. Oxford Management Co., Inc., 137 N.H. 653 (1993).

profits. This is a special relationship indeed.[253]

Meanwhile, "[a] second exception arises where 'an especial temptation and opportunity for criminal misconduct brought about by the defendant, will call upon him to take precautions against it.'" [254] This standard, applied to the social-media-modelled metaverse, provides clear justification for a duty on behalf of platforms to act against third-party harms. As we argued at length in Part II above, platforms building metaverse instances around an audience-monetization model systematically create settings within which novel criminal actions are possible, such as online sexual harassment and the solicitation or extortion of self-generated child sexual abuse materials. These are precisely examples of "especial temptation[s] and opportunit[ies] for criminal misconduct brought about by the (potential) defendant[s]."[255]

2. Attractive Nuisance Doctrine

As early as 1873, the U.S. Supreme Court recognized what would come to be called the doctrine of attractive nuisance, confirming that premises owners have a proactive duty to anticipate that children may trespass where they are not invited, and may not have the maturity to recognize and avoid risks there.[256] As the Louisiana Supreme Court concluded in 1949,

> [O]ne who maintains upon his premises a condition, instrumentality, machine, or other

---

[253] Indeed, one might suggest that, given that the presence of users is essential to creating the sellable data from which the platform is profiting, the relationship of platform to users—including victim and tortfeasor alike—could be analogized as the relationship of employer to employee, or principal to agent. A theory of platform responsibility for third-party harms predicated on treating those third parties as employees or agents of the platform falls outside of the scope of the present Article.

[254] Walls v. Oxford Management Co., Inc., 137 N.H. 653 (1993).

[255] *Id.*

[256] Stout v. Sioux City & P.R. Co., 84 U.S. 657 (1873) (confirming the trial judge's instructions that if the jury found "reason to anticipate that children would be likely to resort to [an unguarded railroad turntable], or that they would be likely to be injured if they did resort to it," the defendants could be found negligent).

> agency which is dangerous to children of tender years by reason of their inability to appreciate the peril therein, and which may reasonably be expected to attract children of tender years to the premises, is under a duty to exercise reasonable care to protect them against the dangers of the attraction.[257]

Even if parental negligence is found to have contributed to the child's presence on a premise where harm befell them, the premise owner may still be found liable for comparative or contributory negligence.[258]

Even someone who does not invite children onto their premises, in other words, is responsible for anticipating that children may arrive, especially if they have done so in the past.[259] The relevance to children's online activities should be clear. Fully thirteen percent of children aged 8-12 in the U.S.—that is, 2.6 million children—have used Snapchat;[260] ten percent of 8-12 year olds—2 million children—have used Instagram;[261] and eight percent of 8-12 year olds—1.6 million children—have used Facebook.[262] Each of these platforms has terms of service

---

[257] Saxton v. Plum Orchards, Inc., 40 So.2d 791, 794 (La. 1949).

[258] *See, e.g.*, Clarke v. Edging, 20 Ariz. App. 267 (Ariz. Ct. App. 1973). For broader discussion, see Evelyn Atkinson, *Creating the Reasonable Child: Risk, Responsibility, and the Attractive Nuisance Doctrine*, 42 L. & SOC. INQUIRY 1122 (2017); Valerie D. Barton, *Reconciling the Burden: Parental Liability for the Tortious Acts of Minors*, 51 EMORY L.J. 877 (2002).

[259] *See, e.g.*, Gatlinburg Construction Co. v. McKinney, 263 S.W.2d 765, 767 (Tenn. 1953) (signaling liability if the owners knew or should have known about the habitual trespass of minors and the attendant risks "which children because of their youth will fail to discover and appreciate"); Ford v. Blythe Bros. Co. 87 S.E.2d 879, 882 (N.C. 1955) (holding against the defendant because the defendant knew that a large number of children were trespassing, even frequently requesting them to leave).

[260] VICTORIA RIDEOUT ET AL., THE COMMON SENSE CENSUS: MEDIA USE BY TWEENS AND TEENS, 2021 at 5 (2022).

[261] *Id.*

[262] *Id*.

excluding users below the age of 13;[263] none of them can plausibly deny awareness of children's usage.[264] Under-age social media usage has grown in step with child ownership of or access to personal devices designed for adults. Already in 2015, eleven percent of eight-year-olds had their own smartphones. By 2021, it was thirty-one percent.[265]

There has been a concurrent rise in children utilizing metaverse technology. As of 2021, one in six children or teens reported having access to a VR headset in their homes.[266] We should not be surprised that in 2021—while Meta's Horizon Worlds was nominally closed to any users under 18—independent researchers found minors present during 66 of 100 five-minute visits they made to the platform.[267] They further report,

> Minors were also spotted in multiple 'Mature Worlds' where Meta permits sexually explicit content, legal drugs, and gambling. Mature Worlds must be marked as 18+ but there are no further safety measures and they are easily accessible from the main menu or in-world 'portals.'
>
> Sexually explicit insults were not uncommon, with researchers encountering four incidents of

---

[263] Sarah Perez, *Snapchat Adds New Teen Safety Features, Cracks Down on Age-inappropriate Conten*t, TECHCRUNCH (Sept. 7, 2023), https://techcrunch.com/2023/09/07/snapchat-adds-new-minor-safety-features-cracks-down-on-age-inappropriate-content/ [https://perma.cc/VUZ4-MKHU]; *Terms of Service*, INSTAGRAM https://help.instagram.com/154475974694511; *How do I report a child under the age of 13 on Facebook?*, FACEBOOK, https://www.facebook.com/help/157793540954833.

[264] *See* evidence reviewed at *supra* note 116; *In re social media*, as discussed in Amanda Hoover, *Omegle Was Forced to Shut Down by a Lawsuit From a Sexual Abuse Survivor*, Wired (Nov. 9, 2023), https://www.wired.com/story/omegle-shutdown-lawsuit-child-sexual-abuse/.

[265] RIDEOUT, *supra* note 260, at 22.

[266] *Id.* at 39.

[267] Center for Countering Digital Hate, *supra* note 183, at 2.

> adults harassing minors in this way. One adult repeatedly shouted at a group of young girls, "I don't want to cum on you," continuing even after the girls said they were minors.[268]

Again, we ask readers who are shocked by our inclusion of such language to consider that we, as adults, have permitted the creation of a world in which exposure to such interactions is commonplace for ten- or eleven- or twelve-year-old children.[269]

Note that the attractive nuisance doctrine has never held that premise owners can or should prevent all conceivable harm to children. Rather, the assessment of liability requires balancing "the burden of eliminating the danger" against "the risk to children involved";[270] the importance of such balancing within premises liability is a topic we return to below. What is expected of premise owners is the exercise of "reasonable care to eliminate the danger or otherwise to protect the children," even children who are trespassing, if their doing so is reasonably foreseeable.[271]

3. Owners' Superior Knowledge and the Constructive Knowledge Standard

Another core element of the premises liability tradition is recognition of owners' superior knowledge: dangerous conditions may exist within a venue that owners or occupiers exercising ordinary care will discover, but which outsiders also exercising ordinary care may not discover until it's too late. This is particularly relevant to digital platforms. Those who design and run social platforms have (vastly) superior knowledge of the levers that can and do shape patterns of interaction within them, including patterns of harmful interaction.[272] Even specialist researchers have close to zero

---

[268] *Id.*
[269] *See* THORN, *supra* note 176.
[270] RESTATEMENT (SECOND) OF TORTS § 339(d).
[271] *Id.* at § 339(e).
[272] VAN DIJCK, *supra* note 106; ARAL *supra* note 98.

insight into the in-platform incidence of harms and risks;[273] ordinary users, relying only on platforms' own self-promotional descriptions, are all the more unaware.[274]

This stands in stark contrast to the knowledge standard applied in Section 230 jurisprudence, which has insisted that constructive knowledge is not adequate to assign platform responsibility, even in cases being pursued under Fight Online Sex Trafficking Act's (FOSTA) explicit carve-out of sexual trafficking cases[275] from Section 230's immunity shield. Passed in 2018, FOSTA aimed to make it possible to hold internet-based communications platforms responsible for hosting user-generated content that facilitates sex-trafficking, including by expanding the possibility of civil liability. The law amended Section 230 to specify that it should not be "construed to impair or limit . . . any claim in a civil action brought under section 1595 of title 18, if the conduct underlying the claim constitutes a violation of section 1591 of that title."[276] However, this wording created an ambiguity over the degree of knowledge required for platform liability. Specifically, Section 1591 sets an actual-knowledge standard for action against third-party actors who benefit from child sex trafficking (defining participation in a venture as "knowingly assisting, supporting, or facilitating a violation of" the statute), while Section 1595 permits civil action "against the perpetrator (or whoever knowingly

---

[273] *Child Safety Online* INTEGRITY INST. (Jan. 19, 2024) https://integrityinstitute.org/blog/child-safety-online [https://perma.cc/S7MW-3FJ9].

[274] *See* Daphne Keller & Max Levy, *Getting Transparency Right*, LAWFARE INST.(July 11, 2022, 9:01 AM), https://www.lawfaremedia.org/article/getting-transparency-right [https://perma.cc/LH2F-SRBE]; *Overview of Online Social Platform Transparency*, INTEGRITY INST. (July 26, 2023), https://integrityinstitute.org/news/institute-news/integrity-institute-releases-overview-of-online-social-platform-transparency [https://perma.cc/3YQX-DXFU].

[275] Fighting Online Sex Trafficking Act, Pub. L. No. 115-164, 132 Stat. 1253 (2018).

[276] Eric Goldman, *The Complicated Story of FOSTA and Section 230*, 17 FIRST AMEND. L. REV. 279 (2019); Lucy Weisner, *Good Intentions and Unintended Consequences: SESTA/FOSTA's First Two Years*, 93 TEMPLE L. REV. 151 (2020).

benefits, financially or by receiving anything of value from participation in a venture which that person knew *or should have known* has engaged in an act in violation of this chapter)."[277] In *Does v. Reddit*, in 2022, the Ninth Circuit ruled that plaintiffs must meet 1591's higher scienter standard in order to proceed without triggering the Section 230 shield.[278]

Applying an actual knowledge standard to assess whether a distributor should be held liable for inadvertently carrying discrete items of defamatory content has stood in our society in good stead to support the fulsome circulation of information, the goal Congress underlined in penning Section 230 three decades ago.[279] That track record argues for maintaining the actual knowledge standard when declining to treat platforms as publishers of third-party speech for purposes of communications torts (defamation, libel, etc.).

However, we suggest that in light of the technological transformations detailed in Part I above, applying a constructive knowledge standard to tortious and criminal conduct in the social-media-modelled metaverse would better achieve Section 230's vision of the internet as a flourishing "forum," where "obscenity, stalking, and harassment by means of computer" is deterred.[280]

One thing that Section 230's supporters argue that the actual knowledge standard has achieved is to mitigate the "moderator's dilemma": the problem that if platforms could be held liable for not removing harmful content once aware of it,

---

[277] 18 U.S.C. § 1591.

[278] Does v. Reddit, Inc., 51 F.4th 1137 (9th Cir. 2022) (resolving FOSTA's 1591/1595 split by saying that plaintiffs must meet the higher scienter requirements of 1591 to proceed without triggering the Section 230 preemption). This may have significant impact on other litigation currently underway, such as Doe v. Mindgeek USA Inc., 2023 WL 8126845 (C.D. Cal. Nov. 17, 2023).

[279] *See* Section 230 *supra*, note 87.

[280] *Id*. at a3 & b5. Item b5 states that it is the policy of the United States "to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer." As we have illustrated with evidence in Section II.D and III.A., in today's social media platform world, undreamt of in 1996 when Section 230 was enacted, the "veil of scale," in effect, precludes criminal law enforcement at the scale necessary to impact the harms underway.

they would be incentivized to avoid seeing it at all. If piercing the 230 shield reinstated the moderator's dilemma, supporters argue, the result would not be better moderation, but no moderation at all.[281]

Yet there is concrete evidence, in documentary and witness testimony, that platforms are already choosing to duck knowledge of the harms they are creating. For instance, Arturo Bejar worked as Facebook's Director of Engineering for Protect and Care up to 2015. When he returned to the company briefly in 2019, he found safety and reporting structures within Instagram had been dismantled even as the platform had grown to include ever-larger numbers of teens and pre-teens. As Senator Blumenthal summarized in a Senate hearing in 2023, Bejar

> resoundingly raised an alarm about statistics showing Facebook's prevalent and pernicious harms to teens telling Mark Zuckerberg, for example, in a memo that more than half of Facebook users had bad or harmful experience, just within the last week. Instead of real reform, he will testify that Facebook engaged in a purposeful public strategy of distraction, denial, and deception. They hid from this committee and all of Congress evidence of the harms that they knew was credible and they ignored and disregarded recommendations for making the site safer and they even rolled back some of the existing protection.[282]

By this evidence, the moderator's dilemma is no longer vanquished; it is alive and well. According to Bejar and his fellow whistleblowers, platforms are choosing to know less rather than more about harms underway on their platforms.[283] Platforms are able to disavow "actual knowledge" because what their human employees create are the highly engineered

---

[281] Goldman, *supra* note 92; Goldman, *supra* note 93.

[282] TECH POL. PRESS, *supra* note 202.

[283] See full range of whistleblowers' testimony and documents in HORWITZ, *supra* note 87.

settings within which certain kinds of interactions are algorithmically favored, targeted, and accelerated. As AI advances, this will be able to be done with ever more precision and ever less human intervention or knowledge.[284]

The legal reasoning that incorporates attention to owners' superior knowledge of their premises has been embraced in premises liability precisely so that venue owners cannot intentionally avoid gaining knowledge of risks in order to duck responsibility. As the Georgia Court of Appeals recently wrote, it is "well established" that proprietors' duty of ordinary care "includes inspecting the premises to discover possible dangerous conditions of which the [proprietor] does not have actual knowledge, and taking reasonable precautions to protect invitees from dangers foreseeable from the arrangement or use of the premises."[285]

For instance, a constructive knowledge standard applied to the social media-modelled metaverse should incentivize more and better deployment of online reporting tools, which research shows are the recourse that children who feel threated or victimized online are most likely to turn to, by far.[286] Bejar argues that better reporting tools are essential to track and reduce platform harm. He also underlines that current, egregious harm could be ameliorated if platforms were forced to acknowledge its existence.

> Instagram is the largest public directory of teenagers with pictures in the history of the world. Meta which owns Instagram is a company where all work is driven by data, but it has been unwilling to be transparent about data regarding the harm that kids experience and unwilling to reduce them. . . . Many have come to accept the false proposition that sexualized content or

[284] Cyphert & Martin, *supra* note 9.

[285] River Place at Port Royal Condo. Ass'n v. Sapp, 856 S.E.2d 28 (Ga. App. Mar. 2, 2021).

[286] *See* THORN, RESPONDING TO ONLINE THREATS: MINORS' PERSPECTIVES ON DISCLOSING, REPORTING, AND BLOCKING (2021), https://info.thorn.org/hubfs/Research/Responding%20to%20Online%20Threats_2021-Full-Report.pdf [https://perma.cc/8EQN-PN8P].

> wanted advances, bullying, misogyny, and other harms are [an] unavoidable evil. This is just not true. We don't tolerate unwanted sexual advances against children in any other public context, and they can similarly be prevented on Facebook, Instagram, and other social media products.[287]

Jurisprudence needs to recognize social platforms' superior knowledge of their own premises as a besetting characteristic of the digital age, rather than allowing a technologically outdated "actual knowledge" standard to incentivize intentional ignorance, and inaction.

4. Balancing Implementation Costs with Value of Prevention

Premises liability does not hold all premise owners liable for all harm that occurs on their premises. Firstly, the injury must be foreseeable.[288] Secondly, case law has developed an imperative to balance value of prevention with attention to the cost of security measures:

> Because landholders are not expected to be guarantors of visitors' safety, a high preventive burden must be justified by high foreseeability and a high harm potential. Obviously, the greatest liability accrues to landholders that fail to take reasonable measures when the burden of doing so is light, when the foreseeability of the harm is high, and when the potential magnitude of the harm is great.[289]

---

[287] TECH POL. PRESS, *supra* note 202.

[288] Trammell Crow v. Gutierrez, 267 S.W.3d 9, 17 (Tex. 2008) (discussing the policy behind the foreseeability requirement).

[289] Jacobs, *supra* note 249. Undertaking a balancing analysis has come to be favored in place of the "open and obvious" standard. *See, e.g.*, Hersh v. E-T Enterprises, Ltd., 752 S.E.2d 336, 342 (W. Va. 2013) (stating "we expressly abolish the open and obvious doctrine in premises liability actions. The obviousness of a danger does not relieve an owner or possessor's duty of care towards others.").

This balancing requires fact-finding. Among the issues that courts consider are: how foreseeable was the third party's conduct in light of the factual circumstances of the case?[290] What security measures does the plaintiff contend the defendant should have implemented to prevent the harm plaintiff suffered? What would the financial and social burden of providing those security measures have been? Given the specific facts regarding the foreseeability of the third party's conduct, would shouldering the expense of the requested security measures have been reasonable?[291] Defendants who can show that their security measures matched industry standards for their business and location are generallyin a strong position to avoid being held liable for third-party harms.

We argue that this balancing is ideal with regard to efforts to reduce foreseeable third-party crime occurring via virtual platforms and is more fit for that purpose than the all-or-nothing liability shield that Section 230 has been taken to confer with regard to third-party "content." If a platform can show that it is following the industry standard of safety measures, and that there are no readily available and affordable measures to significantly reduce harm that it is declining to implement, it will not be found liable for harms that occur in its virtual spaces. That is a standard that the companies building, operating, and profiting from metaverse instances should confidently be able to meet.

C. Other Tort Liability Theories

In recent years, plaintiffs have essayed multiple novel theories of liability for social media harms, the most successful among them, so far, being products liability assertions.[292]

---

[290] *See*, *e.g.*, Timberwalk Apartments, Inc. v. Cain 972 S.W.2d 749 (Tex. 1998) (discussing in detail grounds for assessing the foreseeability of third-party crime).

[291] *See, e.g.*, UDR Tex. Props., L.P. v. Petrie, 517 S.W.3d 98 (Tex. 2017) (reversing the Court of Appeals of Texas because it failed to properly consider whether the risk of harm was unreasonable).

[292] *See e.g.*, Peter Karalis & Golriz Chrostowski, *Product Claims Spike as SCOTUS Ponders Section 230 Fix*, BLOOMBERGLAW (Mar. 2, 2023),

The products liability lawsuits that have most clearly prospered are those where no third-party content or action of any kind are involved. Instead, the allegations specify design features that themselves directly trigger harm or self-harm. This was the case, for instance, with *Lemmon v. Snap, Inc.*, in which plaintiffs were the parents of children who died while speeding over one hundred miles per hour, while using a Snapchat 'speed filter' whose obvious and sole use was to boastfully share evidence that users were driving at high speed.[293] As the court writes,

> [T]he Parents' negligent design claim faults Snap solely for Snapchat's architecture, contending that the app's Speed Filter and reward system worked together to encourage users to drive at dangerous speeds. Notably, the Parents do not fault Snap in the least for publishing Landen's snap. Indeed, their amended complaint fully disclaims such a reading of their claim: 'The danger is not the Snap [message using the Speed Filter] itself. Obviously, no one is harmed by the post. Rather, the danger is the speeding.'[294]

In 2023, over 140 actions brought by school districts and state attorneys general alleging negligent design by Facebook, TikTok, Instagram, YouTube, and Snap were combined into multi-district litigation: *In re social media*.[295] The U.S. District Court of the Northern District of California denied in part the defendants' motion to dismiss, concluding that the "products liability claims . . . do not implicate publishing or monitoring of

---

https://news.bloomberglaw.com/bloomberg-law-analysis/analysis-product-claims-spike-as-scotus-ponders-section-230-fix [https://perma.cc/NF44-8AGY].

[293] Lemmon v. Snap Inc., 995 F.3d 1085, 1088 (9th Cir. 2021).

[294] *Id.* at 1093.

[295] *See* In re Soc. Media Adolescent Addiction/Personal Inj. Prods. Liab. Litig., No. 4:22-md-03047-YGR, 2023 U.S. Dist. LEXIS 203926 (N.D. Cal. Nov. 14, 2023).

third-party content and thus are not barred by Section 230."[296]

Many of the claims the court judged as not barred by Section 230 dealt with dimensions of design that shape users' experience directly: lack of parental controls, lack of options to self-regulate time, addictive design features, and appearance-altering filters.[297] However, the court also allowed multiple claims regarding design failures where bad acts by third-party actors are the implicit source of harm, albeit, the plaintiffs carefully framed their delineation of the defects so as not to make failure to monitor or remove third-party content the crux of the claim. Instead, the allegations include items like "making it challenging for users to report predator accounts and content to the platform" and "not implementing reporting protocols to allow users or visitors of defendants' platforms to report CSAM and adult predator accounts specifically without the need to create or log in to the products prior to reporting."[298]

Meanwhile, a lawsuit against the stranger-pairing site Omegle, which alleged that children were systematically preyed on by adult predators on the site, was allowed by the District Court of Oregon to move forward. The court found that given the open prevalence of sexual solicitation on the site, Omegle's role fit the definition of a service recruiting minors for commercial sex acts and thus fell under the terms of the 2018 Fighting Online Sex Trafficking Act (FOSTA)[299] carveout from Section 230 protection.[300]

However, in other recent cases where the design failings alleged are ones that fail to prevent third-party harm, fewer jurists have been persuaded, and more rulings for plaintiffs

---

[296] *Id.* at *43. In contrast, in a near-simultaneous ruling on a suit brought by school officials in California state courts, the California Superior Court explicitly rejected products liability as a framework for analyzing social media harms. *In re* Coordinated Proceeding Special Title Rule 3.550 Soc. Media Cases, 2023 Cal. Super. LEXIS 76992 (Cal. Sup. Ct. Oct. 13, 2023).

[297] *Id.*

[298] *Id.*

[299] *See* Fighting Online Sex Trafficking Act, Pub. L. No. 115-164, 132 Stat. 1253 (2018).

[300] A.M. v. Omegle.com, LLC, No. 3:21-cv-01674-MO, 2023 U.S. Dist. LEXIS 17581 (D. Or. Feb. 2, 2023). On FOSTA, see Goldman, *supra* note 238; and Citron & Jurecic, *supra* note 238.

reversed.[301] *In re Social Media* remains under appeal and Omegle settled before appeal,[302] but the judgments they occasioned cannot be considered settled law. It is possible that this line of products liability litigation for design choices that fail to hinder third party harm may yet be foreclosed.

We are not aware of any lawsuit yet promulgating a products liability frame with regard to harm in the metaverse, but it will almost certainly happen. Given the central role of wearable physical hardware integrated via proprietary software into immersive metaverse offerings,[303] courts may find products liability a fully plausible theory for claims against device-plus-platform corporate creators within the metaverse, especially with regard to "mixed reality" games that incentivize dangerous real-world acts.[304]

Overall, in sum, products liability/negligent design offers a

---

[301] *See* Brief for Prod. Liab. Advisory Council as Amicus Curiae Supporting Respondents, Gonzalez v. Google, 598 U.S. 617-18 (2023) (arguing that products liability claims in which the cause of harm is third-party content must be dismissed on grounds of Section 230). Ultimately, *Gonzalez v. Google* was remanded to the Ninth Circuit for reconsideration in light of the *Twitter v. Taamneh* ruling, which upheld Twitter's Section 230 immunity. Gonzalez, 598 U.S. at 617-18. *See also, e.g.*, Doe v. Snap, c., No. 22-20543, 2023 U.S. App. LEXIS 33501 (5th Cir. Dec. 18, 2023) (declining to review *en banc* the decision to dismiss claims on the basis of Section 230). For further commentary on *Doe*, see Eric Goldman, *Many Fifth Circuit Judges Hope to Eviscerate Section 230*, TECH. & MKT'G L. BLOG (Dec. 19, 2023), https://blog.ericgoldman.org/archives/2023/12/many-fifth-circuit-judges-hope-to-eviscerate-section-230-doe-v-snap.htm [https://perma.cc/9NWB-7ZB8].

[302] Amanda Hoover, *Omegle Was Forced to Shut Down by a Lawsuit From a Sexual Abuse Survivor*, WIRED (Nov. 9, 2023), https://www.wired.com/story/omegle-shutdown-lawsuit-child-sexual-abuse/ [https://perma.cc/W25M-AHXS].

[303] For instance, there are Meta's MetaQuest headset and co-branded Ray-Ban "smart glasses," the PlayStation from Sony, and the Hololens from Microsoft.

[304] The potential for such harms was made clear during the Pokemon Go craze in 2016, when tales of users being draw into unsafe places or falling off cliffs while pursuing virtual avatars made headlines. Ben Axelson, *Pokemon Go Dangerous? Every Crime, Accident, Death Linked to Game So Far*, SYRACUSE (Jul. 26, 2016), https://www.syracuse.com/us-news/2016/07/pokemon_go_dangerous_every_crime_accident_death_shooting_linked_to_game.html.

model that is well-aligned with some aspects of social media now found to be harmful (image filters that incite dangerous acts; addictive design; inadequate parental controls) and may also have straightforward application for physical harms caused by mixed reality devices. However, with regard to platform liability for systematic incidence of preventable third-party harm, the record of current tort theories is mixed at best. Plaintiffs pursuing products liability frameworks for such harms have gone to great lengths to avoid suggesting that failure to monitor third-party content is what they are alleging. Yet even so, courts have sometimes assessed their claims as doing as exactly that and dismissed them on Section 230 grounds.[305]

Meanwhile, a new kind of claim was advanced in the most recent Massachusetts and Arizona state lawsuits against Meta for harms to children: public nuisance arguments.[306] Given that a common feature of public nuisance enforcement in the physical world is action against locales that become gathering places for third parties engaged in noisy or obstructive conduct, there seems significant potential to use this theory to hold platforms responsible if they foster virtual locales that similarly host repetitive and unaddressed third-party harm.[307] The Massachusetts case currently underway does not, however, attempt to make that case. Rather, what is alleged under the public nuisance count are the harms to children and adolescents' mental health and well-being occasioned by "defendants' psychologically manipulative and exploitative

---

[305] *See, e.g.*, Herrick v. Grindr, 306 F. Supp. 3d 579 (S.D.N.Y. 2018), *aff'd* 765 Fed. Appx. 586 (2d Cir. 2019); Jackson v. Airbnb, Inc., 2022 WL 16753197 (C.D. Cal. Nov. 4, 2022) (dismissing claims against Snap on Section 230 grounds); Doe v. Snap, No. 22-20543, 2023 U.S. App. LEXIS 33501 (5th Cir. Dec. 18, 2023) (declining to review *en banc* the decision to dismiss claims on the basis of Section 230).

[306] Massachusetts v. Meta Platforms, Inc., No. 2384CV02397 (Mass. Super. Ct. Nov. 6 2023); New Mexico v. Meta Platforms, Inc., D-101-CV-2023-02838 (D.N.M. Dec. 5, 2023).

[307] *See* P'SHIP FOR PUB. HEALTH L., OVERVIEW OF NUISANCE LAW 1 (2013), https://www.apha.org/-/media/Files/PDF/factsheets/Overview_of_Nuisance_Law_factsheet.ashx [https://perma.cc/N3WH-5XRU].

design features and tools" (the same harms charged elsewhere in the suit under Unfair and Deceptive Acts and Practices statutes).[308]

Clearly, there is interest from private and public actors, and some judges, in finding a common-law route towards platform accountability for egregious and systemic third-party harms. Also clearly, neither products liability nor public nuisance frameworks currently constitute a silver bullet to achieve that. Recognizing this, we reiterate the importance of premises liability, a framework that is both just and efficient when applied to the social metaverse, as a uniquely apt framework for assessing responsibility for third-party harms shaped by engineered space.

D. Treating Metaverse as Premises Does Not Require Treating Platforms as Publishers

Some scholars and practitioners have argued that Section 230 functions, and should continue to function, as a near-absolute shield against any kind of platform liability for harms committed via social media sites.[309] This would suggest that there is a significant risk that the same reasoning would be extended to the nascent social media/interactive gaming realms of the metaverse, leaving torts and crimes committed there behind the "veil of scale" irremediable and under-deterred. However, recent case law has destabilized the certainty of Section 230's broadest construal, even as hearings and proposals in Congress suggest significant disconformity with 230's functioning.[310]

---

[308] Complaint ¶ 419, Massachusetts v. Meta, No. 2384CV02397.

[309] *See, e.g.*, JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (2019); Eric Goldman, *An Overview of the United States' Section 230 Internet Immunity*, *in* THE OXFORD HANDBOOK OF ONLINE INTERMEDIARY LIABILITY 154 (2020); Jeff Kosseck, *What Was the Purpose of Section 230? That's a Tough Question*, 103 B.U. L. REV. 713 (2023).

[310] *See, e.g.*, Danielle Citron & Benjamin Wittes, *The Internet Will Not Break: Denying Bad Samaritans § 230 Immunity*, 86 FORDHAM L. REV. 401 (2017); Mary Ann Franks, *How the Internet Unmakes Law*, 16 OHIO ST. TECH. L. J. 10 (2020); Cyphert & Martin, *supra* note 8; Danielle Citron, *How*

We are not the first to note the potential relevance of premises liability to this moment of perceived inadequate protection vis-à-vis online harm. In an article in 2021, Kassandra Cabrera noted that "online service providers—against which many brick and mortar businesses continue to compete—have swaddled themselves and their wrongdoing in the blanket immunity granted to them by courts around the country through Section 230."[311] Her proposal is to draw from premises liability in shifting Section 230 jurisprudence to extend a duty of care to online service providers who fail to make good faith efforts to moderate third party content:

> By extending a duty of care to online service providers courts would incentivize the platforms to make risk assessments and engage in cost benefit analyses to determine which safety features to implement. Thus, rather than granting all online services providers immunity, courts would only give immunity in cases where online service providers are treated as publishers, as per the language of Section 230. Further, courts would only impose liability on those providers who have failed to make 'good faith' efforts to moderate content to protect users from foreseeably dangerous third-party content.[312]

As Cabrera notes, "website operators are in the best position to protect their users and have the resources to do so."[313] We certainly would agree with this, but our argument in favor of premises liability goes further. We have traced in detail

---

To Fix Section 230, 103 B.U. L. REV. 713 (2023); Ofchus, *supra* note 205; Lisea, *supra* note 205; Alan Z. Rozenshtein, *Interpreting the Ambiguities of Section 230*, BROOKING INST. (Oct. 26, 2023), https://www.brookings.edu/articles/interpreting-the-ambiguities-of-section-230/ [https://perma.cc/GN5K-ZZ5L].

[311] Kassandra Cabrera, Comment, *Analysis of Section 230 under a Theory of Premise Liability: A Focus on Herrick v. Grindr and Daniel v. Armslist*, 29 U. MIA. BUS. L. REV. 53, 57 (2021).

[312] *Id.*

[313] *Id.*

the ways that platform technology, as shaped by a business strategy reliant on maximizing ease of account formation to speed user growth, has evolved such that social media platforms today are the *only* actors in a position to protect their users. This is already true in non-immersive social media today, and will predictably be true in the metaverse for any platform that follows the same monetization model. The veil of scale precludes either external law enforcement or civil liability for ephemeral and anonymous tortfeasors online. Today's platforms are directly comparable to shadowy premises whose proprietors possess uniquely superior knowledge of risks present, and where child trespassers are known to be frequent, and to sometimes face egregious harm.

The Superior Court of California recently concluded that it is "clear and obvious . . . that the law is unsettled and in a state of development" regarding the exact dimensions and circumstances of Section 230 immunization.[314] They further explained:

> Congress expressed its intention with respect to the preemptive effect of section 230 on state law with a classic "consistent/inconsistent" construct: 'Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.'
>
> (47 U.S.C. § 230(e)(3)). This construct kicks back to the courts to decide whether a state's law including its tort common law is or is not consistent with section 230.[315]

It is our position that courts could plausibly find that the common law of premises liability is in fact consistent with

---

[314] Order Sustaining in Part and Overruling in Part Defendant's Demurrer to Plaintiff's Second Amended Complaint at 2, Neville v. Snap, Inc., No. 22STCV33500 (Super. Ct. Cal. Jan. 2, 2024).
[315] *Id.* at 11.

Section 230 as applied to the metaverse. Recognition of the premises-like dimensions of the social metaverse need not erase respect for the content-conduit role that "interactive computer services" continue to play, nor does it vitiate the Section 230 protections related to that publisher-like role. After all, in the physical world, speech happens in places, and our common law, criminal law, and constitutional law are able to adjudicate accordingly. When a politician holds a rally, we do not absolve event promotors of the responsibility for ensuring that the stands are properly assembled and the venue is not recklessly overcrowded. A publisher's intermediary liability—or lack thereof—vis-à-vis the content of the works they produce can be separated out from premises liability for foreseeable third-party crimes being committed in their office.

Distinguishing between tortious speech and criminal or tortious acts is not trivial—especially not in the virtual world, where every interaction is mediated by transmission. To distinguish between content and conduct requires attention to the specific facts presented. But addressing that distinction is not an unprecedented challenge for our system of law. As scholars have noted, "crime does not receive First Amendment protection merely because it is in the guise of speech."[316] Common examples include bribery offers and conspiracies.[317] In the metaverse, as discussed above, crimes committed in the form of communication will likely include fraudulent taking of (virtual) property and sexual solicitation of minors.

The premises-like dimensions of modern social media platforms are particularly prominent in the metaverse, where immersive and experiential interactions with people or products—rather than text or other speech-like content per se—are at the core of what the platform provides. Meta itself declares, on a banner headline at about.meta.com, that "[t]he metaverse provides new ways to connect and share

---

[316] Benjamin Means, *Criminal Speech and the First Amendment*, 86 MARQ. L. REV. 501, 507 (2002).

[317] *See, e.g.*, MODEL PENAL CODE § 5.03(1) (1962) (criminal conspiracy); *id.* §§ 248.8, 240.1 & 240.3- 240.7 (offering to pay or receive a bribe); *id.* § 211.3 (threatening another person with severe harm).

experiences."[318] Given the specific structural and functional similarities between metaverse instances and built spaces of social encounter in the physical world, the longstanding common law of premises torts is a wellspring of insight into questions of risk, harm, and measured redress here.

Indeed, we would suggest that relying on tort liability is a better shield against government overreach and a stronger protector of the freedom to innovate than many of the other public responses to online harm being promoted. Better to make metaverse platforms acquire (virtual) premises liability insurance—just as brick-and-mortar businesses having been buying premises liability insurance policies for over a century[319]—and let insurers codify evolving baseline expectations for underwriting, than to rely on government regulators or legislators to keep up with the rapidly shifting possibilities of online harm.

Conclusion

For decades, social media companies have built their platforms on a model that offers free and near-frictionless account creation to users who create and run spaces of engagement that can be algorithmically promoted to other users. This is the very same model that is currently set to predominate in extensive realms of the coming metaverse as well.

This route to growth has systematically enabled the privatization of profits and the socialization of costs. Fundamentally, opportunities for virtual harm scale at the speed and low cost of all kinds of digital expansion. The institutional apparatus of accountability (e.g., police, courts, etc.) does no such thing. As a result, our current environment provides a system in which most actors committing harms in

---

[318] *The Metaverse*, META, https://about.meta.com/metaverse/ [https://perma.cc/SW3S-BNEN].

[319] Jim Robertson, *How Umbrella Policies Started Part 1: Early Liability Coverage*, INT'L RISK MGMT. INST. (Mar. 1, 2000), https://www.irmi.com/articles/expert-commentary/how-umbrella-policies-started-part-1-early-liability-coverage [https://perma.cc/5RXB-MS7K].

the metaverse face no rational expectation of consequences. And for their part, the digital platforms shaping the opportunities for harm have—under traditional readings of Section 230—little incentive to balance the risks they create against their shareholder-driven mandate for growth. The predictable result is underinvestment in preventive measures.

Yet, we have argued, jurists can respect the protective shield offered by Section 230 with regard to third-party *speech*, without foreclosing inquiry into harms created by third-party *acts*. The same technological trends that have stretched the platforms-as-content-conduits model to the breaking point, we have argued, have rendered a platforms-as-premises model a useful complement to it.

Harms exist in online spaces; there is public demand to reduce them. Yet given the opacity and complexity of the array of platform design decisions that shape outcomes,[320] there is good reason to doubt that external micromanaging via regulatory apparatus will efficiently achieve the desired harm reduction.

It is as a framework to adjudicate harms and incentivize risk reduction in the metaverse *today*, without need for governmental micromanaging or speech-constraints, that we believe premises liability shines. As with traditional, physical premises, if a platform has constructive knowledge that the design of their place creates predictable and egregious harms, that platform should take reasonable, industry-standard steps to reduce risk to the people they invite into that venue—including the child trespassers who are drawn into the "premises" that these owners have created—or face liability.

---

[320] *See* Gillespie, *supra* note 33; Kou & Gui, *supra* note 138.