WHAT ARE YOU LOOKING AT?
EMERGING PRIVACY CONCERNS WITH EYE TRACKING IN VIRTUAL REALITY

RICHARD KOCH*

* J.D. Candidate, University of Colorado, Class of 2023; B.A., Fordham University, Class of 2018. This paper is dedicated to my friend and former clinic partner, Stacey Weber. In addition to introducing me to the topic of this paper, Stacey served as an invaluable mentor and soundboard throughout my time in law school. Without her support, this paper would not exist. I also want to express my gratitude to the faculty and staff at Silicon Flatirons, both past and present. I owe particular thanks to Professors Margot Kaminski, Blake Reid, Kristelia García, and Amie Stepanovich, as well as our Student Coordinator, Sara Schnittgrund—Silicon Flatirons' true beating heart. To the extent that a reader finds this article useful or intriguing, then all the credit is due to them. All mistakes are my own.

INTRODUCTION

Did you know that you are a mildly neurotic closeted homosexual that holds numerous adverse biases towards members of other races? You are also recovering from a recently suffered concussion, have a strong predilection for gambling, and will likely develop Parkinson's disease in roughly 30 to 40 years (sorry). Oh, and before I forget, you also draw very positive associations (93rd percentile among your demographic group, in fact) with in-game advertisements that display the color yellow. Allow me to introduce myself: my name is Meta, and it is great to get to know you. Thank you for using the Meta Quest Pro, our newest virtual reality headset offering built-in eye-tracking capabilities. Did I mention you have beautiful irises?

The phrases "the eyes are the window to the soul" and "I see it in your eyes" certainly sound like poetic cliches. However, a growing body of research indicates looking into someone's eyes might be closer to an exercise in mind reading.[1] From a scientific and technical standpoint, the ability to analyze someone's eyes and learn their innermost thoughts and feelings is no longer just a theoretical possibility. Eye-tracking is becoming a widely deployed feature in

1. *See* discussion *infra* Section I.B.

many commercial virtual reality (VR) headsets, and it may be ubiquitous in the very near future.[2]

This note explores how the implementation of eye-tracking in virtual reality headsets raises novel biometric privacy concerns, specifically as it relates to information revealed from tracking individual eye activity. Virtual reality and eye-tracking technologies are expected to experience a significant uptick in consumer adoption over the coming years.[3] Due to the wide range of sensitive information that can be revealed by analyzing a person's eye activities,[4] we may see a new—and potentially lucrative—market emerge for the collection, analysis, and resale of eye-tracking data to third party advertisers.

Eye-tracking information was not contemplated by lawmakers during the crafting of many privacy laws. As a result, it does not fit squarely within existing definitions of biometric data under existing U.S. legal frameworks.[5] This gap threatens the privacy interests of all VR users in the U.S., which in the coming years may number in the hundreds of millions. These privacy risks could be best addressed by a joint private-public effort between federal legislators and the VR industry itself.

First, this note provides a survey of the types of sensitive information that can be disclosed by analyzing a person's eye activities, including: sexual preferences, biometric identification, moods and emotions, inferences of cultural affiliation and identity, and predispositions to diseases and medical conditions. Second, it turns to the current state of the VR industry within the U.S., discussing its history, adoption and market value, incorporation of eye-tracking technologies, and business relationship with the advertising industry. This note then peeks into the future, attempting to predict how these aspects of VR may evolve in the near future, with a special emphasis placed on the emergence of the "Metaverse" concept—the 3D world considered to be the next iteration of the internet. This note proceeds to discuss the potential privacy risks posed by these developments, including their underlying philosophical justifications, and follows with an examination of the shortcomings of the U.S. regulatory framework currently governing eye-tracking data. Lastly, this note discusses possible governmental and private sector reform measures, including an analysis of their respective upsides

2. *See* discussion *infra* Sections II & III.

3. *Id.*

4. *See generally* Jacob L. Kröger et al., *What Does Your Gaze Reveal About You? On the Privacy Implications of Eye Tracking.*, 576 IFIP ADVANCES IN INFO. AND COMMC'N TECH. 226, 227 (2020), https://doi.org/10.1007/978-3-030-42504-3_15 [https://perma.cc/GXW7-6Z7L].

5. *See* discussion *infra* Section V.

and downsides, considered from the points of view of consumers, legislators, and the VR industry. Legislators and industry alike are currently at a crossroads regarding how best to balance the competing interests of innovation, profit, privacy, and practicality. A joint private-public approach based on transparency, consent, and cooperation is the best option for doing so.

I. INFERENCES FROM THE EYES: WHAT EYE-MOVEMENTS CAN REVEAL ABOUT A PERSON THROUGH ADVANCED INFERENTIAL ANALYTICS

In March 2020, a team of German academics published a meta-analysis on the types of information that can be revealed by analyzing a person's eye activities.[6] The study drew "from a range of scientific disciplines, including neuroscience, human-computer interaction, medical informatics, affective computing, experimental economics, psychology, and cognitive science," and represents a useful starting point for categorizing the types of sensitive gaze data that can be collected within virtual environments.[7] According to the paper, eye-tracking data can provide insight into a user's "biometric identity, mental activities, personality traits, ethnic background, skills and abilities, age and gender, personal preferences, emotional state, and physical and mental health condition."[8] Before delving into the specifics, however, it is necessary to provide a general technical overview of how eye-tracking works in the context of virtual environments.

A. Technical Overview of Eye-Tracking Within Virtual Reality

At present, VR environments exist in two main forms: "(1) so-called 'CAVEs' (Cave Automatic Virtual Environments) and (2) 'HMDs' (head-mounted displays)."[9] HMDs are the more common form among commercial applications. They use an HMD together with a computer and a head tracker; inside the HMD the user is "shown two screens, one for each eye, to provide stereo images."[10] The technical process for using eye-tracking in HMD's is complex.

6. *See* Kröger et al., *supra* note 4, at 227.

7. *Id.*

8. *Id.*

9. Martin Meißner et al., *Combining Virtual Reality and Mobile Eye Tracking to Provide a Naturalistic Experimental Environment for Shopper Research*, 100 J. BUS. RSCH. 445, 446 (2019).

10. *Id.* at 447.

Nonetheless, it can be neatly summarized for the purpose of providing a working understanding. According to Bhavisha Ravi, a former Technology Attorney at Alston Bird, eye-tracking is accomplished within HMD environments by:

> [E]mploying near-infrared technology along with a [high- resolution] camera to track a person's gaze. In this process, the light is directed toward the center of the eyes, creating reflections in the cornea. These reflections are tracked using a camera. This technology can determine the places on a document or image that your eyes fixated on ("gaze points"), the amount of time spent in those places, if the eyes locked toward a specific object ("fixation") and the movements from one fixation to another (also known as "saccades.")[11]

The accuracy of the data "depends on the hardware used but, also, on the quality of the mapping between gazes and the objects fixated in the environment (either on the desktop, the 3D model in the VR or the physical reality in the field)."[12] The eye tracker must be calibrated by the programmer in order to learn this mapping, and if the calibration is weak, "the quality of the recorded data will suffer and thus the interpretation of the fixated objects might be wrong."[13] In many applications, eye data are "condensed into fixations that approximate the focus of attention," and when ordered in time on a computer, the "sequence of fixations sequence comprises [what is called] a 'scanpath.'"[14] Scanpath data may be "coupled with details about the underlying stimuli (e.g., areas of interest displayed on screen), creating a richer notion of both what was attended to and how attention varied."[15]

Information collected from eye trackers can be combined with other individual sensors built into HMDs, such as "movement sensors, EEG and brain-computer interfaces (BCIs), and other pressure and fitness sensors."[16] Additionally, "bodily motions, and the

11. Bhavishya Ravi, *Privacy Issues in Virtual Reality: Eye Tracking Technology*, BLOOMBERG L. (June 3, 2017), https://www.alston.com/-/media/files/insights/publications/2017/07/alstonbird-eyetracking-16pvlr27.pdf [https://perma.cc/Q9BK-8GZX].

12. Meißner et al., *supra* note 9, at 450.

13. *Id.*

14. Daniel J. Liebling & Sören Preibusch, *Privacy Considerations for a Pervasive Eye Tracking World*, PROC. OF THE 2014 ACM INT'L JOINT CONF. ON PERVASIVE AND UBIQUITOUS COMPUTING 1169, 1170 (2014).

15. *Id.*

16. JOSEPH JEROME & JEREMY GREENBERG, FUTURE PRIV. F., AUGMENTED REALITY + VIRTUAL REALITY: PRIVACY & AUTONOMY CONSIDERATIONS IN EMERGING, IMMERSIVE DIGITAL WORLDS 17 (2021), https://fpf.org/wp-content/uploads/2021/04/FPF-ARVR-Report-4.16.21-Digital.pdf [https://perma.cc/G2QY-JUB4].

relationship between different body movements and segments, can serve as a tracking mechanism."[17] Altogether, spending twenty minutes in VR can generate approximately two million data points and unique recordings of body language.[18] These sensors and recordings both improve HMD functionality and enhance user experience. For example, VR companies may use a "detailed map of our bodies to allow us to interact realistically using avatars" and "sensory data about physiological responses to apps . . . in order to rate games and to detect and fix errors making people sick."[19] In addition, companies might "track where [our] eye moves in order both to prevent dizziness and to optimize display and rendering."[20] Used together, these data points allow developers to "understand key areas of focus and thereby influence how [to] design an experience; how [to] play with a user's attention and 'direct' for them in a medium which is not restricted to a simple frame."[21]

Importantly, eye-tracking data differs from other signals of human activity because it is "largely involuntary and unconscious."[22] Considering how fleeting glances and pupil dilation are extremely difficult, if not impossible to consciously regulate, "gaze and associated data like blinks and pupillometry" are unique insofar as they are "not fully under volitional control."[23] As a result, one commentator argues, "if a company is collecting [eye tracking] data, you won't know."[24] This may raise ethical concerns regarding the extent

17. *Id.*

18. *See* Jeremy Bailenson, *Protecting Nonverbal Data Tracked in Virtual Reality*, 172 J. AM. MED. ASS'N PEDIATRICS 905, 905 (2018).

19. Mark A. Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 U. PA. L. REV. 1051, 1125–26 (2018).

20. *Id.*

21. Sol Rogers, *Seven Reasons Why Eye Tracking Will Fundamentally Change VR*, FORBES (Feb. 5, 2019), https://www.forbes.com/sites/solrogers/2019/02/05/seven-reasons-why-eye-tracking-will-fundamentally-change-vr/?sh=7c7aeb023459 [https://perma.cc/YRG7-GAWM].

22. Avi Bar-Zeev, *The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail*, VICE (Mar. 28, 2019), https://www.vice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail [https://perma.cc/UGF2-QCQT].

23. Liebling & Preibusch, *supra* note 14, at 2.

24. Bar-Zeev, *supra* note 22. Alternatively, while a company may disclose this collection practice under a traditional notice-and-choice, or "click-through" consent model, it is unlikely users would read or comprehend it. While outside the scope of this paper, the phenomenon of "consent theater" resulting from information overload is briefly discussed *infra* Section IV.B.i. For further discussion of the topic, *see* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J. L. & POL'Y FOR INFO. SOC'Y 543, 544, 564 (2008); *see also* Solon Barocas & Helen Nissenbaum, On Notice: The Trouble with Notice and Consent (Oct. 2009) (unpublished manuscript), https://nissenbaum.tech.cornell.edu/papers/On%20Notice%20-%20The%20Trouble%20with%20Notice%20and%20Consent.pdf [https://perma.cc/MKU2-P8TQ].

to which VR users are "filmed unintentionally by the scene camera of a mobile eye tracking system,"[25] a subject discussed in greater detail in the sections ahead.

B. Types of Personal Information That Can Be Revealed Through Eye Activity

Studies across disciplines show eye tracking in VR, revealing "how and certainly at what people gaze," can provide a "wealth of understanding" into the human condition.[26] This knowledge spans the full gamut of human cognition and can produce extremely intimate, granular insights at the individual level. Further, if the data were aggregated and processed within machine learning models, the resulting patterns could also be used to make inferences about people whose data were not even collected.[27] In sum, eye tracking in VR allows companies to "know us better than we know ourselves, to an unprecedented degree . . . to predict, with potentially even more accuracy than before, what we think, how we feel, and how we will act, even before we are aware of it."[28]

For one, studies show that gaze characteristics, much like fingerprints, are unique for every individual and can thus be exploited for biometric identification.[29] More specifically, people can be identified "based on distinct patterns of pupil reactivity and gaze velocity" and also by the "complex textures and color patterns in a person's iris," known as iris recognition.[30] While not usually advertised, commercial eye trackers "often record and process high-resolution images of the user's iris, which can not only be used to uniquely identify the user but also to deceive iris-based authentication mechanisms and thereby steal the user's identity."[31]

25. Meißner et al., *supra* note 9, at 451.

26. Liebling & Preibusch, *supra* note 14, at 2.

27. *See, e.g.*, Alicia Solow-Niederman, *Information Privacy and the Inference Economy*, 117 NW. L. REV. 357, 361 (2022); Antonio Rizzo, et al., *A Machine Learning Approach for Detecting Cognitive Interference Based on Eye-Tracking Data*, 16 FRONTIERS IN HUMAN NEUROSCIENCE 1 (2022).

28. *When Your Eyes Betray You: Is Virtual Reality Too Close for Comfort?*, LONDON SCH. ECON. BLOG (June 13, 2017), https://blogs.lse.ac.uk/medialse/2017/06/13/when-your-eyes-betray-you-is-virtual-reality-too-close-for-comfort/ [https://perma.cc/5K4J-F5WU].

29. *See generally* Virginio Cantoni et al., *Gaze-Based Biometrics: An Introduction to Forensic Applications*, 133 PATTERN RECOGITION LETTERS 54 (2018).

30. Kröger et al., *supra* note 4, at 228.

31. *Id.* at 229 (citing Brendan John et al., *EyeVEIL: Degrading Iris Authentication in Eye Tracking Headsets*, PROC. 11TH SYMP. ON EYE TRACKING RSCH. & APPLICATIONS, No. 37, 2019, at 1.

Eye tracking data can also be used to infer personality traits.[32] One study found "characteristics [of eye activity] that capture rich temporal information on visual behavior seem to convey fundamental information related to all personality traits, and consistently outperform classic characteristics that have been isolated for investigation in laboratory situations, such as fixation duration."[33] The study found the "importance of characteristics varies for different personality traits. For example, pupil diameter was important for predicting neuroticism but was less useful for predicting other traits."[34] Relatedly, studies show "intercultural differences are reflected in certain gaze characteristics."[35] "Those studies suggest that people of different cultural backgrounds are found to exhibit discriminative eye-movement patterns when seeking information on search engine results pages, when exploring complex visual scenes, and when viewing videos of actors performing cultural activities."[36] Other eye tracking research observed "test subjects view 'other-race faces' differently than faces of their 'own race' in terms of the facial features scanned," while a separate study found "characteristic changes in pupil size, which are attributed to elevated cognitive effort during face recognition, when people look at 'other-race faces.'"[37]

Characteristic eye movement patterns also reveal personal information about diseases and medical conditions, such as "concussion, fetal alcohol syndrome, chronic pain, Alzheimer's disease, Parkinson's disease," depression, and schizophrenia.[38] Eye tracking has been further used to "examine preferences for certain types of gambling, mobile apps, activities of daily living" and extensively in the study of love and sexual desire.[39] For instance, researchers have "analyzed pupillary responses and the allocation of visual attention

32. Sabrina Hoppe et al., *Eye Movements During Everyday Behavior Predict Personality Traits*, 12 FRONTIERS IN HUM. NEUROSCIENCE 1 (2018).

33. *Id.* at 6.

34. *Id.*

35. Kröger et al., *supra* note 4, at 230; *See, e.g.*, Hannah F. Chua et al., *Cultural Variation in Eye Movements During Scene Perception*, 102 PROC. NAT'L ACAD. SCI. 12629 (2005); Joshua O. Goh et al., *Culture Modulates Eye-Movements to Visual Novelty*, 4 PUB. LIB. SCI. ONE 1 (2009); Mari-Carmen Marcos et al., Cultural Differences on Seeking Information: An Eye Tracking Study (July 24, 2013) (CHI '13: CHI Conference on Human Factors in Computing Systems, Paris, France, Apr. 27–May 2, 2013), https://www.semanticscholar.org/paper/Cultural-differences-on-seeking-information%3A-an-eye-Marcos-Garc%C3%ADa-Gavilanes/22529cc5c3ed967e601f9836f62acf052978414b [https://perma.cc/XA7N-W9GN].

36. Kröger et al., *supra* note 4, at 230.

37. *Id.*

38. *Id.* at 233.

39. *Id.* at 232.

to measure levels of sexual arousal and to investigate mating preferences towards specific facial characteristics, age groups, body shapes, body parts, and signs of social dominance."[40] In addition, by analyzing neural systems underlying pupil dilation and spontaneous blink rate, researchers found that eye tracking can reveal "crucial aspects of cognitive processing, such as attention, working memory, decision making, and cognitive control, across age groups."[41]

This list of sensitive information represents a mere glimpse into a much larger picture, and it will likely be a subject of increasing interest to researchers as VR grows in popularity.[42] Whether commercial applications of VR collect and monetize any of the above data streams is not yet known. However, seeing as eye-tracking information may be particularly valuable in the VR advertising context, the incentives to do so are strong.[43] According to Tobii, the world's leading manufacturer of eye tracking technology, VR headsets equipped with eye tracking "are ideal for understanding behavior, delivering accurate insights about a person's attention, intent, and how they react to events. Its application is essentially limitless."[44]

II. CURRENT STATE OF COMMERCIAL VR TECHNOLOGY: HISTORY, FUNCTIONALITY, BUSINESS MODEL, AND DATA COLLECTION PRACTICES

Eye tracking has been around since 1908, when scientist Edmund Huey built a device used to "track eye movement during the reading process."[45] In these early stages, eye tracking was primarily used for research and scientific purposes. By the end of the

40. *Id.*

41. Maria K. Eckstein et al., *Beyond Eye Gaze: What Else Can Eyetracking Reveal About Cognition and Cognitive Development?*, 25 DEVELOPMENTAL COGNITIVE NEUROSCIENCE 69, 87 (2017).

42. *See, e.g.*, Jooyoung Kim, *Advertising in the Metaverse: Research Agenda*, 21 J. OF INTERACTIVE ADVERT. 141, 143 (2021) (stating that the Journal of Interactive Advertising will "soon announce a call for special issue articles focusing on advertising in the metaverse").

43. *See* discussion *infra* Section III.C.

44. *XR Headsets: Get a Boost with Eye Tracking*, TOBII, https://www.tobii.com/products/integration/xr-headsets [https://perma.cc/HBB3-PA7P]; Ankit N. Sing, *4 Most Popular Eye Tracking Softwares in the Market*, MEDIUM (Aug. 20, 2019), https://ankitnsingh.medium.com/4-most-popular-eye-tracking-softwares-in-the-market-c8755c4da2e5#:~:text=Tobii%20Pro%20Lab,it%20comes%20to%20eye%20tracking [https://perma.cc/8KQN-HX4D]

45. Tom Sharman, *Is Eye Tracking the Future of Virtual Reality?*, MEDIUM (July 3, 2020), https://medium.com/virtual-library/is-eye-tracking-the-future-of-virtual-reality-c5af7b0763f3 [https://perma.cc/Z68Z-3D22].

1990's, however, advertising agencies began using it to "observe reactions to internet content (animated graphics, navigation buttons, online advertisements.)"[46] Portending its application in today's VR, the main driver was "the growing potential of the online products and services market."[47]

In recent times, eye tracking has been approached with a mix of excitement and concern. In the VR context, one journalist in 2013 described it as both an advertising "goldmine," promising to provide an "enormous amount of value in knowing what groups of people paid attention to which types of ads," while also decrying it as an "entirely new [method] of invasive data collection and tracking."[48] In 2014, researchers from Microsoft offered a similar mixed prediction at the 2014 ACM International Joint Conference on Pervasive and Ubiquitous Computing. The paper presented at the conference, self-described as a "first step towards a privacy impact assessment of eye tracking," ultimately concluded that the "benefits of pervasive eye tracking [were] vast."[49] It also cautioned VR practitioners to be "conscious of . . . exposing . . . users to unintentional privacy leaks" and take a "minimal approach" to data processing and sharing in order to moderate privacy risks.[50] Either way, "pervasive eye tracking [was] likely to become reality."[51]

As of 2022, nine years after publication of Microsoft's research, the global VR, augmented reality (AR), and mixed reality (MR) market was estimated at 30.7 billion USD.[52] In terms of usage, estimates predicted 52.1 million people would use VR and 83.1 million people would use AR at least once per month in 2020 in the U.S. alone, representing, respectively, 15.7% and 25.0% of the U.S. population.[53] VR gaming and VR video comprised the largest consumer

46. *Id.*

47. *Id.*

48. Tarun Wadhwa, *Eye-Tracking Technologies Are About to Make Advertising Even More Invasive*, FORBES (May. 8, 2013, 11:45 AM), https://www.forbes.com/sites/tarunwadhwa/2013/05/08/with-recent-advances-in-eye-tracking-advertising-set-to-become-even-more-invasive/?sh=1fb882352a0c [https://perma.cc/Q6C9-ZE8G].

49. Liebling & Preibusch, s*upra* note 14, at 2, 8.

50. *Id.* at 8.

51. *Id.*

52. Nikhil Pachhandara, *Looking Forward to The Future Of AR, VR, And MR*, FORBES (Apr. 25, 2022, 7:45 AM), https://www.forbes.com/sites/forbestechcouncil/2022/04/25/looking-forward-to-the-future-of-ar-vr-and-mr/?sh=771d906265ca [https://perma.cc/H8E7-AJ59].

53. Victoria Petrock, *US Virtual and Augmented Reality Users 2020*, EMARKETER: INSIDER INTEL. (Apr. 7, 2020), https://www.emarketer.com/content/us-virtual-and-augmented-reality-users-2020 [https://perma.cc/8CBZ-JVCK].

use cases for all VR technology.[54] The global eye tracking market was estimated at $368 million that same year.[55] Notably, eye tracking technology is characterized as a significant "growth opportunity" for VR due to its "ability to offer an enhanced experience to the users, improve image quality, helping eyes to reduce strain and improve focus."[56] Some industry experts even describe the technology as "essential and foundational" to VR's future.[57]

In July of 2019, however, only three VR headsets offering built-in eye tracking were available in the commercial marketplace: the HTC VIVE Pro Eye, Pupil Labs, and the Varjo VR-1.[58] That same year, Henrick Eskillson, then CEO of Tobii, remarked in an interview that the technology was still ramping up to ubiquitous deployment.[59] While the company was "working with the majority of manufacturers on incorporating eye tracking" at the time, Eskillson did not expect their product "to hit the real consumer volumes" until 2021.[60]

Eye tracking has been used for VR advertising purposes since at least 2017. HTC used it to "see whether the ads [were] being viewed or if users [were] turning away their gaze," allowing their advertisers to "better target the desired audiences."[61] Another company, Looxid Labs, ran a similar eye tracking experiment to "track

54. Thomas Alsop, *Augmented and Virtual Reality (AR/VR) Forecast Spending Worldwide in 2020 (in Billion U.S. Dollars), by Segment*, STATISTA (Sept. 22, 2022), https://www.statista.com/statistics/737615/ar-vr-spending-worldwide-by-segment/ [https://perma.cc/7MG4-FGEX].

55. *Eye Tracking Market with COVID-19 Impact Analysis by Offering (Hardware, Software, Services), Tracking Type (Remote and Mobile), Application (Assistive Communication, and Human Behavior & Market Research), Vertical, and Geography- Global Forecast to 2025*, MKTS. AND MKTS. (July 20, 2020), https://www.marketsandmarkets.com/Market-Reports/eye-tracking-market-144268378.html?gclid=Cj0KCQjwwY-LBhD6ARIsACvT72NMiV2oyHz-iENS4QaUzn4oI-RoLdb7XPA6PGQfB0rfJ5N1CaryMlxMaArwuEALw_wcB [https://perma.cc/3NU7-JXC3].

56. *Id.*

57. Demond Cureton, *Hand and Eye-Tracking: XR Today Expert Round Table*, XR TODAY (July 27, 2022), https://www.xrtoday.com/mixed-reality/hand-and-eye-tracking-xr-today-expert-round-table/ [https://perma.cc/5ZNP-WGBS] (interviewing Johan Hellqvist, Head of XR Segment at Tobii and Ben Cathart, Product Marketing Manager at Varjo Technologies).

58. Andrew Beall, *Is Now the Time to Buy a VR Headset With Built In Eye Tracking?*, WORLDVIZ (July 25, 2019), https://www.worldviz.com/post/is-now-the-time-to-buy-a-vr-headset-with-built-in-eye-tracking [https://perma.cc/T8VL-SC7E].

59. *See* Scott Stein, *Eye Tracking is the Next Phase for VR, Ready or Not*, CNET (Jan. 31, 2020), https://www.cnet.com/tech/mobile/eye-tracking-is-the-next-phase-for-vr-ready-or-not/ [https://perma.cc/238D-RYS5].

60. *Id.*

61. Christopher Dring, *HTC Introduces Eye-Tracking VR Ads*, GAMES INDUS. (Mar. 31, 2017), https://www.gamesindustry.biz/articles/2017-03-31-htc-introduces-eye-tracking-vr-ads [https://perma.cc/YX5G-FU43].

[users] emotional responses" and glean insights "based on [user] emotional reactions to VR experiences."[62] Given that VR companies "often reserve the right to collect and disseminate all the information they might possibly want to, knowing that consumers rarely read (let alone comprehend) the legalese they agree to," other companies likely engaged in this practice as well.[63]

Professor Brittan Heller calls this practice "biometric psychography"—a modern phenomenon of combining biometric data with predictive behavioral analytics.[64] In 2016, this practice was considered a "relatively new and promising development" steadily progressing towards commercial viability.[65] Today, however, eye tracking manufacturers publicly champion such uses for their products. Tobii's website, for example, proudly proclaims:

> Everyone wants to know how their consumers *truly think and feel*. With eye tracking, you can see through their eyes. Whether you want to visualize the impact of your shopper journey, packaging design, *advertising*, or user experience, attention data is unbiased and empowers you to attract more customers.[66]

Eye tracking will soon be a commonplace feature in commercially available VR headsets. The adoption will be driven by the value of the personal information that can be gleaned therefrom, the technical improvement and enhanced user experience, and the growing global investment in the "Metaverse" concept. As predicted in 2013, eye tracking may usher in a "whole new world of interaction and control," where, simply from observing our eyes within virtual environments, advertisers understand us better than we understand ourselves.[67]

62. Lucas Matney, *Looxid Labs is Combining Brain Waves and VR to Build an Analytics Super Engine*, TECHCRUNCH (Sept. 18, 2017, 6:51 PM), https://techcrunch.com/2017/09/18/looxid-labs-is-combining-brain-waves-and-vr-to-build-an-analytics-super-engine/ [https://perma.cc/3ACF-ZWEE].

63. Diane Hosfelt, *How Much is That New VR Headset Really Sharing About You?*, MOZILLA MIXED REALITY BLOG (Dec. 20, 2019), https://blog.mozvr.com/vr-headset-data-collection/ [https://perma.cc/T552-W69H].

64. Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 VAND. J. ENT. & TECH. L. 1, 4 (2020).

65. Simon Parkin, *Nvidia's Eye-Tracking Tech Could Revolutionize Virtual Reality*, MIT TECH. REV. (July 21, 2016), https://www.technologyreview.com/2016/07/21/245354/nvidias-eye-tracking-tech-could-revolutionize-virtual-reality/ [https://perma.cc/8W3Y-3UZX].

66. *Consumer Research and User Experience*, TOBII (emphasis added), https://www.tobiipro.com/applications/marketing-user-research/ [https://perma.cc/7U54-YDGJ].

67. Wadhwa, *supra* note 48.

III. FUTURE OF COMMERCIAL VR TECHNOLOGY: NEW CAPABILITIES AND MARKETS FOR BIOMETRIC EYE-MOVEMENT INFORMATION

Estimates project the global AR, VR, and MR market reaching USD $300 billion as soon as 2024.[68] The global eye tracking market is projected to double within a similar period, forecasted to reach over USD $1 billion by 2025.[69] According to Heller, the drive towards consumer adoption of VR will "likely incorporate the sale of user data to third parties" and "more and more features to delve into the physical and emotional states of [VR] users, creating a demand for [eye tracking data]."[70] The underlying rationale is simple: "the ability to tell advertisers more about their targeted audience—including what they pay attention to, what their emotional state is upon viewing or interacting with products, and personal characteristics about their health and well-being—is a lucrative offer."[71] Consumer adoption of advanced VR is largely driven by the promise of the Metaverse.

A. The Metaverse: What It Is, and Why It's The "North Star" of Eye Tracking Technologies

The Metaverse can be defined as a "unified 3D virtual world where users can conglomerate via their digital selves (i.e., avatars) and perform complex interactions."[72] Originally envisioned by science fiction writer Neal Stephenson as a metaphor of the real world, it aspires to provide a "new place to interact with other humans and bots to play games, conduct business, socialize and shop" and, in doing so, "redefine our entire relationship with the internet."[73] As

68. Pachhandara, *supra* note 52.

69. Press Release, OMNIVISION, OMNIVISION and Tobii Join Forces on Eye Tracking to Drive the Vision of Metaverse (Jan. 5, 2022), https://www.ovt.com/press-releases/omnivision-and-tobii-join-forces-on-eye-tracking-to-drive-the-vision-of-metaverse/ [https://perma.cc/NA3T-PVKZ].

70. Heller, *supra* note 64, at 36–37.

71. *Id.* at 37.

72. *Who is Building the Metaverse? A Group of 160+ Companies, and You*, XR TODAY (Dec. 7, 2021), https://www.xrtoday.com/virtual-reality/who-is-building-the-metaverse-a-group-of-160-companies-and-you/ [https://perma.cc/KGU7-9WMV]; As a minor qualification, note that there is no industry consensus on how exactly the Metaverse should be defined or described. For a comprehensive discussion of the subject, *see* Kim, *supra* note 42, at 142–43.

73. Veronica Combs, *The Metaverse: What Is It?*, TECHREPUBLIC (Oct. 29, 2021), https://www.techrepublic.com/article/metaverse-what-is-it/ [https://perma.cc/8WFY-57PC]; Scott Stein, *Why 2022 Could Be the Year to Create Your Avatar and Join the Metaverse*, CNET (Dec. 30, 2021, 4:00 AM), https://www.cnet.com/tech/computing/why-2022-could-be-the-year-to-create-your-avatar-and-join-the-metaverse/ [https://perma.cc/C6RN-A3ZN].

of December 2021, over 160 companies operating across seven different vertical markets were reported to be building the Metaverse together.[74] Meta, formerly known as Facebook, "pledged to spend USD $10 billion a year over the next decade" and "rivals such as Apple and Microsoft are also pursuing similar aims that Big Tech executives describe as part of the next evolution of the internet."[75] Even Bill Gates is on board, predicting in his annual year-in-review letter that the Metaverse will host a majority of U.S. office meetings "…within the next two to three years."[76]

Eye tracking technology will be essential to realizing the Metaverse's full immersive potential.[77] Combined with other features, such as face tracking and AI, eye tracking will be used in VR to "capture emotions and reactions and translate them into avatar animations" and "enhance and optimize graphics through a process called foveated rendering, which allows [a user] to choose things in VR by just glancing at them."[78] Tobii has even described the Metaverse as the company's "north star."[79]

B. The Metaverse Becoming a Reality

Tobii and OmniVision Technologies, a Chinese digital products developer, announced on January 5, 2022, a "jointly developed eye-tracking reference design" to "advance solutions for vision in the Metaverse."[80] The venture intends to "help extended reality original equipment manufacturers . . . speed time to market for high demand XR consumer electronics products."[81] Three months prior,

74. *Who is Building the Metaverse? A Group of 160+ Companies, and You*, *supra* note 72. Non-profit academic institutions are also getting involved on the periphery of the Metaverse. *See, e.g.*, *Metaverse Collaborative*, N.Y.U. SCH. PRO. STUD., https://www.sps.nyu.edu/homepage/metaverse.html [https://perma.cc/V7SE-59B9].

75. Hannah Murphy, *Facebook Patents Reveal How It Intends to Cash in on Metaverse*, FIN. TIMES (Jan. 17, 2022), https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647 [https://perma.cc/9K3M-NHRP].

76. Tom Huddleston Jr., *Bill Gates Says the Metaverse Will Host Most of Your Office Meetings Within 'Two or Three Years' — Here's What It Will Look Like*, CNBC (Dec. 9, 2021, 1:10 PM), https://www.cnbc.com/2021/12/09/bill-gates-metaverse-will-host-most-virtual-meetings-in-a-few-years.html [https://perma.cc/92WS-YZ7T].

77. *See, e.g.*, Johan Hellqvist, *Eye Tracking – Making the Metaverse Authentic*, TOBII BLOG (Feb. 10, 2021), https://www.tobii.com/blog/eye-tracking-making-the-metaverse-authentic [https://perma.cc/9CYC-PEWT] ("[P]roper communication in the metaverse will only work if devices come equipped with eye tracking.").

78. Stein, *supra* note 59.

79. Dean Takahashi, *How Tobii Is Expanding Eye Tracking to New Markets*, VENTUREBEAT (Aug. 8, 2021, 8:45 AM), https://venturebeat.com/2021/08/08/how-tobii-is-expanding-eye-tracking-into-new-markets/ [https://perma.cc/L2RJ-7AM5].

80. OMNIVISION, *supra* note 69.

81. *Id.*

Tobii announced another high-profile partnership with VR hardware manufacturer Pimax Innovation, aiming to "make eye tracking a standard feature . . . in the upcoming generation of Pimax's high-end headsets."[82] According to the press release, the partnership provides "further evidence of eye tracking as a foundational technology in the future of XR headsets" and helps "bring the full potential of the Metaverse close[r] to consumers."[83]

Three major players were "widely expected" to release VR headsets with built-in eye tracking by the end of 2022: Meta, Sony, and Apple.[84] Thus far, the only company to deliver is Meta, who announced its Meta Quest Pro headset just this past month, on October 11, 2022.[85] Starting at USD $1,499, the Meta Quest Pro headset includes five inward-facing cameras used for "real-time expression tracking" ("Smiles, eye-brow raises, winks and all.").[86] According to the accompanying Eye Tracking Privacy Policy, "abstracted gaze data is generated in real time on [the] headset, and processed on device or Meta servers." [87] The data will not be used for biometric identification.[88] Apple's forthcoming headset, however, is rumored to offer iris scanning for both payment and identity authentication purposes.[89] Sony's website does not indicate

82. *Tobii and Pimax Announce New Partnership to Bring Eye Tracking to Consumer Virtual Reality Headsets*, PR NEWSWIRE (Oct. 22, 2021, 11:06 AM), https://www.prnewswire.com/news-releases/tobii-and-pimax-announce-new-partnership-to-bring-eye-tracking-to-consumer-virtual-reality-headsets-301406712.html [https://perma.cc/67K6-X8Y6].

83. *Id.*

84. *See* Stein, *supra* note 59; Roland Moore-Colyer, *PSVR2 – Release Date, Price Specs, Games, and More*, TOM'S GUIDE (updated Feb. 22, 2023), https://www.tomsguide.com/news/psvr-2-release-date-price-new-controllers-leaks-and-latest-news [https://perma.cc/6REC-NMCB]; Jon Fingas, *Apple's Mixed Reality Headset Reportedly Uses Iris Scanning for Payments and Sign-Ups*, ENGADGET (Oct. 14, 2022, 11:30 AM), https://www.engadget.com/apple-mixed-reality-headset-iris-scanning-153036223.html [https://perma.cc/VT8J-NMJ2].

85. Meta Quest (@MetaQuestVR), TWITTER (Oct. 11, 2022, 11:43 AM), https://twitter.com/MetaQuestVR/status/1579890489402314754?cxt=HHwWhMC-zfGB8-wrAAAA [https://perma.cc/7KQB-BTUQ].

86. *This is Meta Quest Pro (Tech Specs)*, META, https://www.meta.com/quest/quest-pro/tech-specs/#tech-specs [https://perma.cc/8ZJ9-P4V6]; Khari Johnson, *Meta's VR Headset Harvests Personal Data Right Off Your Face*, WIRED (Oct. 13, 2022, 7:00 AM), https://www.wired.com/story/metas-vr-headset-quest-pro-personal-data-face/ [https://perma.cc/EZD7-SM6M].

87. *Eye Tracking Privacy Notice*, META, https://www.meta.com/help/quest/articles/accounts/privacy-information-and-settings/eye-tracking-privacy-notice/ [https://perma.cc/THK8-JL4V].

88. *Id.* ("Eye tracking is not used to identify you.")

89. *See* Fingas, *supra* note 84.

whether or not the PS VR2 headset (expected to be released in 2023) will use eye tracking for biometric identification.[90]

Patent filings illustrate the creative ways companies plan to monetize these new capabilities. According to *Financial Times*, Meta has patented "multiple technologies that wield users' biometric data in order to help power what the user sees," including one that "explores how to present users with personalized advertising in augmented reality, based on age, gender, interest and how the users interact with a social media platform."[91] Another patent, granted on January 4, 2022, "lays out a system for tracking a user's facial expression through a headset that will "adapt media content" based on those responses."[92] These filings illustrate how VR companies "intend to cash in on [the] virtual world, with hyper-targeted advertising and sponsored content that mirrors its existing USD $85 billion-a-year ad-based business model."[93] Following the reports, Meta commented: "While we don't comment on specific coverage of our patents or our reasons for filing them, it's important to note that our patents don't necessarily cover the technology used in our products and services."[94]

Recalling a journalist's July 2020 statement that, "eye tracking won't become a staple in the mainstream technology space until a big player like Facebook [sic] or Google focus their attention on it," it appears that time is now. [95]

C. Potential Advertising (Ab)Uses for VR Eye Tracking Data

Eye tracking in VR has been described as the "holy grail" of advertising.[96] The raw metrics provided by eye trackers create a unique "psychographic profile . . . of your personality and your predicted future behavior," which, in effect, allows advertisers to "learn how you regard any visually-represented idea: cars, books, drinks, food, websites, political posters and so on."[97] In practical applica-

90. *Playstation VR2*, PLAYSTATION, https://www.playstation.com/en-gb/ps-vr2/ [https://perma.cc/ZT98-38PR] ("The PS VR2 headset detects the motion of your eyes, allowing for heightened emotional response and enhanced expression when meeting fellow players online.").

91. Murphy, *supra* note 75.

92. *Id.*

93. *Id.*

94. *Id.*

95. Sharman, *supra* note 45.

96. Bar-Zeev, *supra* note 22.

97. *Id.*

tion, eye tracking can provide advertisers with "even more opportunities to make money from your choices—and your *indecision*—effectively serving up these insights and impulses to those who want to sell you things, at the exact right time and place."[98] Economic forces within the gaming industry will accelerate this trend. For instance, because advertising provides an "important source of revenue for the developer," using data to predict players external purchasing needs "will become increasingly necessary as more games become free-to-play."[99]

As the Metaverse expands and our "interactions with companies and their applications move from screens in our hands to headsets on our faces,"[100] the potential market for collecting and reselling eye tracking data will likely expand in tandem. A new mode of marketing may emerge where VR companies routinely exploit the "wealth of information" revealed through eye tracking for "targeted advertising at a very granular level."[101] Thus, as one commentator puts it, it is "not hard to imagine a world in which [companies in the Metaverse] give advertisers information on where our eyes are focused to help them better measure our attention, target us with ads, and compel us to buy stuff."[102]

Meta's Eye Tracking Privacy Policy for the Quest Pro does not explicitly state the company will use this data for marketing. Rather, it merely helps Meta to "personalize your experiences."[103] This saying is a common industry euphuism; targeted advertisements are coming to the Metaverse.[104] Nick Clegg, Meta's head of global affairs, arguably confirmed as much back in 2021, stating in an interview: "For us, the business model in the metaverse is commerce-led . . . clearly ads play a part in that."[105]

98. *Id.*

99. Joe Newman, "*Press Start to Track?": Privacy and the New Questions Posed by Modern Video Game Technology*, 42 AIPLA Q.J. 527, 567 (2014).

100. Tatum Hunter, *Surveillance Will Follow Us into 'the Metaverse,' and Our Bodies Could Be Its New Data Source*, WASH. POST (Jan. 13, 2022, 8:00 AM), https://www.washingtonpost.com/technology/2022/01/13/privacy-vr-metaverse/ [https://perma.cc/D6NP-CEE9].

101. Davit Uberti, *Come the Metaverse, Can Privacy Exist?*, WALL ST. J. (Jan. 4, 2022), https://www.wsj.com/articles/come-the-metaverse-can-privacy-exist-11641292206 [https://perma.cc/2EXV-D6HV].

102. Hunter, *supra* note 100.

103. *Eye Tracking Privacy Notice*, *supra* note 87.

104. *See generally* Tami Kim et al., *Why Am I Seeing This Ad? The Effect of Ad Transparency on Ad Effectiveness*, 45 J. CONSUMER RSCH. 906, 908 (2019) (noting that "well-targeted ads are objectively more personalized"); Thomas Germain, *Meta's New Headset Will Track Your Eyes for Targeted Advertising*, GIZMODO (Oct. 13, 2022, 3:14 PM), https://gizmodo.com/meta-quest-pro-vr-headset-track-eyes-ads-facebook-1849654424 [https://perma.cc/264D-FEAE].

105. Murphy, *supra* note 75.

Outside of the consumer sphere, employers in the Metaverse might increasingly rely on eye tracking to "monitor our behavior and even our minds."[106] For example, companies might want to "determine whether [employees] [are] 'paying enough attention' during virtual presentations at work, or even to try to measure [prospective employee's] cognitive load during job interviews."[107] Human resources departments already use VR for employee assessment and training.[108] The extent to which employers source and measure candidate eye-tracking activity is not known, but it is listed as a metric that can be used in the assessment process.[109] Tobii continues to explore "how you take eye-tracking or attention . . . and create insights around people."[110] The company intends to deliver these insights "through mass market types of applications or mass market products" and continue research into corresponding "definitions of signals and needs."[111] In addition to third party marketing partners, such "insights" and "signals" could be "delivered" to prospective employers.

Regardless of the context in which they are ultimately used, eye tracking data gleaned from virtual environments will be "exploited in ways that cause ramifications in real life."[112] One such ramification is wide-scale privacy risk. The following section explores this risk and the various types of harms it can cause.

IV. PRIVACY RISKS POSED BY EYE TRACKING TECHNOLOGIES IN VR

Privacy was first conceptualized by the U.S. legal system as "the general right of an individual to be let alone."[113] In 1967, Pro-

106. Davit Uberti, *supra* note 101.

107. Hunter, *supra* note 100.

108. *See, e.g.*, *Virtual Recruitment*, VIRTUAL REALITY EXPERIENCES, https://www.virtualrealityexp.co.uk/virtual-recruitment/ [https://perma.cc/98UL-EZSE]; Mark Whittle, *Leveraging VR Technology for Developing Your HR Strategy*, MEETINVR, https://www.meetinvr.com/2020/11/01/leveraging-vr-technology-hr-strategy/ [https://perma.cc/EEL6-QP85] (describing how VR interviewees become "become so immersed in the VR world that they forget to self-monitor and their true behaviors and attitudes are revealed").

109. *See Virtual Recruitment*, *supra* note 108 ("We are able to arrange additional selection activities using the headset so that your virtual interviews can be combined with group activities or other assessments relevant to important job-related competencies.").

110. Takahashi, *supra* note 79.

111. *Id.*

112. Ray Walsh, *Virtual Reality Face Tracking Causes Serious Privacy Concerns*, PROPRIVACY (Mar. 16, 2021), https://proprivacy.com/privacy-news/new-htc-virtual-reality-sensors-raise-privacy-concerns [https://perma.cc/49UY-KU9V].

113. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy* 4 HARV. L. REV. 193, 205 (1890).

fessor Alan Westin further refined the term as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others"—a definition which, in turn, prompted legislative privacy reforms both domestically and across the world.[114] In modern parlance, privacy embraces a wide range of understandings and is closely tied to concepts such as personhood, autonomy and control, intimacy, and relationship management.[115] As such, the meaning of privacy can vary depending upon the context in which it is invoked. Consider how perspectives might change depending on whether one is in their bedroom or walking down a public street; whether a parent is listening to their child through a bedroom door or an F.B.I. agent is surveilling a suspected terrorist's email account; or whether one is in the impartial physical world or immersed in a commercially rendered virtual one.

A. The Contextual Integrity Framework of Privacy and the Typology of Privacy Harms

Recognizing the context-dependent nature of privacy, this note discusses privacy primarily through Helen Nissenbaum's framework of Contextual Integrity, which conceptualizes privacy as being about appropriate flows of information, where the appropriateness is defined by the context and its contextual informational norms.[116] Contextual Integrity, thus, focuses on appropriate flows of information "relative to the stakeholders within a specific context who are trying to achieve a common purpose or goal."[117] In application, the framework aims to:

> . . . evaluate whether or not the informational norm is legitimate, worth defending, and morally justifiable. This includes looking at the stakeholders and analyzing who may be harmed and who is benefitting from any informational exchange. Then looking to see whether or not it diminishes any political or human rights principles like the diminishment of

114. ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1967).

115. For discussions of autonomy and control, personhood, intimacy, and relationship management theories of privacy, *see generally* Jeffrey H. Reiman, *Privacy, Intimacy, and Personhood*, 6 PHIL. & PUB. AFF. 26 (1976); Dong-Joo Lee et al., *Managing Consumer Privacy Concerns in Personalization: A Strategic Analysis of Privacy Protection*, 35 MGMT. INFO. SYS. Q. 423 (2011).

116. *See generally* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE (2010).

117. Kent Bye, *Primer on the Contextual Integrity Theory of Privacy with Philosopher Helen Nissenbaum*, VOICES OF VR (June 24, 2021), https://voicesofvr.com/998-primer-on-the-contextual-integrity-theory-of-privacy-with-philosopher-helen-nissenbaum/ [https://perma.cc/99YR-4XV7].

> the freedom of speech. And then finally evaluating how the information exchange is helping to serve the contextual domain's function, purpose, and value.[118]

With this framework in mind, we turn to the ways in which eye tracking in VR can expose individuals to an array of discrete privacy harms. As a normative foreground, a recent study found strong consumer preferences *against* expansive use or sharing of eye tracking and other biometrically VR-derived data.[119]

While privacy harms "have been a challenge to conceptualize because they are so varied," professors Danielle Citron and Daniel Solove offer a useful typology for the purposes of this note.[120] According to their work, privacy harms can be categorized into seven different types, including: "(1) physical harms; (2) economic harms; (3) reputational harms; (4) psychological harms; (5) autonomy harms; (6) discrimination harms; and (7) relationship harms."[121] In November 2021, the Global Initiative on Ethics of Extended Reality (XR) called for a "focus on defining harms within extended reality that result when personal digital privacy is breached."[122] The following section explores two of these harms: autonomy and discrimination.

B. As Applied: Eye Tracking Data and Privacy Harms

1. Autonomy Harm: Manipulation

According to Citron and Solove, autonomy harms "involve restricting, undermining, inhibiting, or unduly influencing people's choices" whereby "people are either directly denied the freedom to decide or are tricked into thinking that they are freely making choices when they are not."[123] Manipulation is a sub-type of autonomy harm involving "undue influence over a person's behavior or

118. *Id.*

119. *See* Jessica Outlaw et al., *"Don't Track My Life" Virtual and Augmented Reality Consumer Data & Privacy Survey*, EXTENDED LIFE (Nov. 17, 2021), https://www.extendedmind.io/survey [https://perma.cc/M697-V5B6].

120. Danielle K. Citron & Daniel Solove, *Privacy Harms*, 102 B.U. L. REV. 793, 830 (2022).

121. *Id.* at 831.

122. MARK MCGILL, IEEE STANDARDS ASSOCIATION, THE IEEE GLOBAL INITIATIVE ON ETHICS OF EXTENDED REALITY (XR) REPORT: EXTENDED REALITY (XR) AND THE EROSION OF ANONYMITY AND PRIVACY 15 (2021), https://standards.ieee.org/wp-content/uploads/import/governance/iccom/extended-reality-anonymity-privacy.pdf [https://perma.cc/P5CZ-PPSZ].

123. Citron & Solove, *supra* note 120, at 845.

decision-making."[124] Ryan Calo contends that manipulation creates both "subjective privacy harm insofar as the consumer has a vague sense that information is being collected and used to her disadvantage, but never truly knows how or when and objective privacy harms to consumers" and, also, "objective privacy harm when a firm uses personal information to extract as much rent as possible from the consumer."[125] Stripped to its core, the privacy harm of manipulation "is that it can violate people's autonomy (by making them instruments of another's will) and offend their dignity (by failing to treat them with respect)."[126]

Eye tracking in VR gives companies the power "to alter a user's perception of reality" and "open the possibility of real-time manipulation, nudging, and abuse both of individuals and at a societal level."[127] Specifically, user behaviors or thoughts "could be anticipated and consequently manipulated to the benefit and desire of a third party (the XR platform, applications on that platform, governments, etc.), which undermines the right to agency, or reverse engineering fixed action patterns."[128] In the words of Kurt Opsahl, Deputy Director of the Electronic Frontier foundation, "social VR platforms or third-party developers may be tempted to use [eye tracking data] . . . to make emotionally manipulative content that subtly mirrors the appearance or mannerisms of people close to us, perhaps in ways we can't quite put our fingers on."[129] Autonomy harms may also extend beyond the temporal present. For example, "once [eye tracking] data has been captured by said third parties, further processing and insight into user[s'] lives and behaviors might be generated far into the future."[130] Autonomy harms are further complicated by issues of individual consent and comprehension.

Privacy policies generally allow businesses to "use and disclose personal information however they'd like unless the consumer opts

124. Citron & Solove, *supra* note 120, at 846.

125. Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1029 (2014).

126. Cass R. Sunstein, *Fifty Shades of Manipulation*, 1 J. MKTG. BEHAV. 213, 217 (2015).

127. MCGILL, *supra* note 122, at 10.

128. *Id.* at 10–11.

129. Kurt Opsahl & Katitza Rodriguez, *Your Avatar is You, However You See Yourself, and You Should Control Your Experience and Your Data*, ELEC. FRONTIER FOUND. (Jun. 2, 2021), https://www.eff.org/deeplinks/2021/06/your-avatar-you-however-you-see-yourself-and-you-should-control-your-experience-0 [https://perma.cc/EJZ4-CX8E].

130. MCGILL, *supra* note 122 at 11; *see* Solow-Niederman, *supra* note 27 at 361 (describing how "insights about an individual can be derived from aggregations of seemingly innocuous data . . . that individuals may not have even realized they were disclosing").

out, [thereby] emphasizing the role of individual choice."[131] While effective in theory, this model of notice-and-consent, or "click-through" consent, is broken in practice. Academics observe that "users may have difficulty discerning the identities of third party affiliates with whom gaming companies share data even after reading the relevant privacy policies," and even if they do, "the use of big data analytics precludes non-experts from understanding many [relevant] privacy implications."[132] Even assuming that a policy is read in full, "most people do not understand how involuntary bodily indicators of emotional responses, mental state, or health can disclose fundamentally private information, such as truthfulness, inner feelings, and sexual arousal."[133]

2. Autonomy Harm: Chilling Effect

Chilling effects, another sub-type of autonomy harm highlighted in Citron and Solove's typology, involve "harm caused by inhibiting people from engaging in certain civil liberties such as free speech, political participation, religious activity, free association, freedom of belief, and freedom to explore ideas."[134] In effect, the "monitoring of communications can make people less likely to engage in certain conversations, express certain views, or share personal information."[135]

According to Heller, using eye tracking data to "enrich existing commercial profiles" creates a "risk of self-censorship…in the most fundamental way."[136] In the commercial context, users may "find themselves trying to limit what they feel, think, or express for fear that information will be monetized or researched."[137] The risk of government surveillance warrants greater concern. The issue is well illustrated by Mozilla's Diane Hosfelt, rhetorically asking: "Are we prepared to give up the ability to make decisions without constantly worrying that the government is monitoring our eye-track-

131. Diane Hosfelt, Making Ethical Decisions For The Immersive Web 7 (May 14, 2019) (working paper), https://arxiv.org/pdf/1905.06995.pdf [https://perma.cc/4EAC-72S7].

132. N. C. Russell et al., *Privacy in Gaming*, 29 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 61, 86 (2020); Hosfelt, *supra* note 131, at 7.

133. Heller, *supra* note 64, at 33; *see* Solow-Niederman, *supra* note 27, at 386–87 (quoting Sandra Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioral Advertising*, 35 BERKELEY TECH. L.J. 367, 370, 376–77 (2020)).

134. Citron & Solove, *supra* note 120, at 854.

135. *Id.*

136. Heller, *supra* note 64, at 33.

137. *Id.*

ing data [and thereby] revealing [our] internal thought processes?"[138] Given eye activity is largely subconscious, even if a user wanted to "self-censor or hide his or her preferences [he or she] would not be able to."[139] Thus, eye tracking "may change the fundamental nature of [VR] and put users on guard for self-censorship of their innermost thoughts, feelings, and emotions."[140]

3. Discrimination Harms

Discrimination often involves curtailment of autonomy, but it differs insofar as it "involves unequal treatment that creates shame and stigma as well as societal consequences of further entrenching disadvantages to marginalized groups."[141] Discrimination "creates harm far beyond lost opportunities; it leaves a searing wound of stigma, shame, and loss of esteem that can turn into permanent scars."[142]

As explained in Section I, eye tracking can reveal a wealth of information about an individual's sexual preferences and identity, attitudes and predispositions concerning race, religious beliefs, and even their own ethnic composition.[143] Individuals who could face discrimination based on "sex, race, sexual orientation or certain health conditions may generate observed biometric data that could be used to infer this information without their consent."[144] Consequentially, the mass adoption of eye tracking in VR "could be significant and devastating [if] used for the purposes of discrimination and profiling in reality."[145]

To illustrate this point, consider how "[eye tracking derived] information that divulges a user's sexual identity could present real harms in parts of the world where . . . LGBTQ status is legally persecutable."[146] Similar data could also be used to populate virtual interactions based on inferred racial or gendered preferences, thereby "reinforcing existing bias toward "'othered' groups . . ."[147] In other words, biometric identification could make it possible for a

138. Hosfelt, *supra* note 131, at 7.
139. Heller, *supra* note 64, at 33.
140. *Id.* at 32.
141. Citron & Solove, *supra* note 120, at 855.
142. *Id.*
143. *See* discussion *supra* Section I.
144. ELLYSSE DICK, INFO. TECH. & INNOVATION FUND, BALANCING USER PRIVACY AND INNOVATION IN AUGMENTED AND VIRTUAL REALITY 17 (Mar. 8, 2021), https://itif.org/publications/2021/03/04/balancing-user-privacy-and-innovation-augmented-and-virtual-reality/ [https://perma.cc/2UGC-FG6K].
145. MCGILL, *supra* note 122, at 9.
146. JEROME & GREENBERG, *supra* note 16, at 18.
147. MCGILL, *supra* note 122, at 11.

VR user "to get tagged with a permanent digital 'kick me' sign attached to their digital back."[148]

V. EXISTING LAWS AND REGULATIONS FOR PRIVACY IN XR

There are no legal safeguards that explicitly govern the use, collection, and resale of eye tracking information under existing U.S. law. As a result, the current system of digital privacy protection may "no longer [be] tenable in an extended reality world."[149]

A. National Privacy Laws

The U.S. does not have a single, comprehensive federal law regulating the collection and use of personal data in general nor biometric data in particular. Instead, the privacy regulatory landscape can be characterized as a "patchwork of national and state-level legislation" addressing sector-specific and data-specific concerns.[150] For example, the Children's Online Privacy Protection Act (COPPA), the Family Educational Rights and Privacy Act (FERPA), and the Health Insurance Portability and Accounting Act (HIPAA) regulate children's personal information, educational records, and health information, respectively. Other federal laws protect financial information and banking records, video viewership information, and government-held records.[151]

In addition to these sectoral laws, the Federal Trade Commission (FTC) functions as a sort of ombudsman regulator of consumer privacy. Pursuant to Section 5 of the FTC Act, which empowers the agency to pursue "unfair or deceptive acts or practices in or affecting commerce," the FTC has brought enforcement actions against a range of companies for issues such as deceptive privacy policies and unfair data collection/use practices.[152]

While the FTC and the sector-specific federal laws *do* regulate data that may be gathered in extended reality, these regulations "only address specific purposes of information, rather than more general information types."[153] As a result, the current federal regulatory scheme is out of scope for addressing emergent eye tracking privacy concerns in any meaningful way.

148. JEROME & GREENBERG, *supra* note 16, at 21.

149. MCGILL, *supra* note 122, at 15.

150. DICK, *supra* note 144, at 18.

151. *See* Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801–6809, §§ 6821–6827; Video Privacy Protection Act of 1988, 18 U.S.C. § 2710; Privacy Act of 1974, 5 U.S.C. § 552a.

152. 15 U.S.C. § 45(a)(1) (1914); *Privacy and Security Enforcement*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement [https://perma.cc/Z7EW-BEF4].

153. DICK, *supra* note 144, at 18.

B. State Biometric Privacy Laws

Several state laws regulate personal information generally and biometric data specifically. In 2008, Illinois became the first U.S. state to enact a biometric privacy law, the Biometric Information Privacy Act (BIPA).[154] Since then, four states adopted legislation modeled on BIPA and twenty-seven others "had BIPA-modeled legislation pending as of June 2021."[155]

Described as the "nation's most robust and litigated biometric law," Illinois's BIPA employs two separate definitions for "biometric identifier" and "biometric information."[156] The statute defines "biometric identifier" as "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry" and "biometric information" as "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier *used to identify an individual* [not including] information derived from items or procedures excluded under the definition of biometric identifiers."[157] Professor Britan Heller highlights "two problematic constraints" embedded in these statutory definitions:

> First, they rely on narrow physiological categories of data that may not cover data captured in immersive systems. Legislators may not have previously contemplated this type of information as having important privacy implications, so it is reasonable that it was not included before the emergence of immersive technology. Second, and even more importantly, such data is only covered if it is "for authentication purposes." This second constraint creates a huge loophole—physiological data used to determine a person's likes, interests, or motivations, rather than their identity, is almost certainly not covered. While there is limited opportunity to capture this data from non-immersive technology, the richness of immersive environments and data capture creates ample opportunity to leverage data in novel ways.[158]

154. 740 ILL. COMP. STAT. ANN. 14/1–14/99 (LexisNexis 2022).

155. The four states that have passed BIPA-modeled legislation include Arkansas, California, Texas, and Washington. *See* ARK. CODE ANN. § 4-110-101–108 (2022); CAL. CIV. CODE § 1798.100–120 (Deering 2020); TEX. BUS. & COM. CODE § 503.001 (2022); WASH. REV. CODE § 19.375.010–040 (2022). For a list of the twenty-seven states with pending biometric legislation, *see* Christopher Ward & Kelsey C. Boehm, *Developments in Biometric Information Privacy Laws*, FOLEY & LARDNER (June 17, 2021), https://www.foley.com/en/insights/publications/2021/06/developments-biometric-information-privacy-laws [https://perma.cc/JH4R-9TGL].

156. Heller, *supra* note 64, at 34; 740 ILL. COMP. STAT. ANN. 14/10.

157. 740 ILL. COMP. STAT. ANN. 14/10 (emphasis added).

158. Heller, *supra* note 64, at 35–36.

These definitional shortcomings—or at best, statutory grey zones—are readily apparent when considering their applicability to recently released, or soon to be released, commercially available VR headsets. For instance, it seems likely that data derived from Apple's forthcoming VR headset would fall under both statutory definitions, given that it is collected by scanning a person's irises (biometric identifier) and used for the purpose of verifying the person's identity (biometric information).[159] Data derived from Meta's Quest Pro, however, is probably not captured as "biometric information," given that it is purportedly *not* used for identification purposes. Similarly uncertain is whether Meta's eye tracking technology would constitute an "iris or retina scan," given the traditional understanding of the terms. Looking forward, it remains "unclear whether a court would decide that new concepts related to biometrics are strictly limited to identity or if biometric psychography is an expansion of the concept."[160]

C. Case Law: The Fourth Amendment & The Third-Party Doctrine

> [T]ime works changes, brings into existence new conditions and purposes. Subtler and more far-reaching means of invading privacy have become available to the government. […] Advances in the psychic and related sciences may bring means of exploring *unexpressed beliefs, thoughts and emotions*. […] Can it be that the Constitution affords no protection against such invasions of induvial security?[161]

Another important area of privacy law implicated by eye tracking data is government surveillance and law enforcement activity. The Fourth Amendment provides to U.S. citizens against the government "the right . . . to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[162] In the 1970s, however, the Supreme Court decided two landmark cases that created a noteworthy exception to this fundamental protection, known today as the Third-Party Doctrine.[163] The doctrine holds

159. *See* Fingas, *supra* note 84 (describing features rumored to be included in Apple's new VR headset).

160. Heller, *supra* note 64, at 36.

161. Olmstead v. United States, 277 U.S. 438, 473–74 (1928) (Brandeis, J., dissenting) (emphasis added) (internal quotation marks omitted).

162. U.S. CONST. amend. IV.

163. *See generally* United States v. Miller, 425 U.S. 435 (1976); Smith v. Maryland, 442 U.S. 735 (1979).

that a person has no legitimate expectation of privacy in information that he or she voluntarily turns over to a third party: once a person does so, Fourth Amendment protection no longer applies.[164]

Eye tracking data likely falls within the scope of the Third-Party Doctrine exception. Specifically, because VR users must voluntarily agree to a company's privacy policy and terms of service in order to use the product, it follows that "any information collected or processed in an AR or VR environment that is not processed locally could be obtained by police in response to a legal request."[165] In other words, your reasonable expectation of privacy in VR-derived data is forfeited by the act of "providing" it to the company who sold you the headset.

Nonetheless, in light of the 2018 Supreme Court decision *Carpenter v. United States*, some commentators express optimism that the scale and sensitivity of VR derived data could serve as a catalyst for reconsideration of the doctrine.[166] In *Carpenter,* the Court confronted "how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals."[167] The Court declined to "extend *Smith* and *Miller* to cover these novel circumstances," reasoning, due to "the unique nature of cell phone location records, the fact that the information is held by a third party does not by itself overcome the user's claim to Fourth Amendment protection."[168]

One interpretation of *Carpenter* is the Supreme Court "appears to be acknowledging that technological advances may require extending constitutional protections over data that had previously been treated as non-private and accessible to government authorities."[169] Perhaps the "data generated by XR experiences could prove a good candidate."[170] As of this writing, a reasonable search produces no judicial decisions implicating the Fourth Amendment and VR-derived information.

164. *See* Miller, 425 U.S. at 443 (1976) (". . . the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities").

165. JEROME & GREENBERG, *supra* note 16, at 18.

166. *Id.*

167. Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018).

168. *Id.* at 2217.

169. JEROME & GREENBURG, *supra* note 16, at 18.

170. *Id.*

D. Transatlantic Regulation: The GDPR

VR eye tracking data collection practices by U.S. companies also implicate international data privacy regimes, such as the European Union's General Data Protection Regulation (GDPR). Unlike the U.S.'s sectoral approach, the GDPR creates strong legal protections for individual rights, limits processing and collection of sensitive data, and places a particular emphasis on special categories of data (such as biometric data). Importantly, it also imposes obligations on any company that collects biometric data from individuals within the EU, regardless of the location of the company itself.[171] A California company processing the biometric data of an individual in Brussels, for example, would be captured by the law.

The GDPR requires controllers to have a "lawful basis" for processing personal data, typically by seeking consent or by determining a "legitimate interest" in the processing.[172] Therefore, "many of the potential privacy violating activities [regarding biometrically-derived data in VR] are not ruled out by default by GDPR, but rather . . . would have to be justified through garnering user consent or building a legal case for the allowance of said activity."[173] The consent standard weakens the GDPR's ability to adequately protect VR-derived data. As Heller explains:

> The illusion of consent can be particularly tricky in the case of immersive technology, where such data collection may be necessary for it to function . . . This is especially the case with technology like the HMDs used by AR and VR, which require eye tracking and sensors to effectively operate.[174]

Currently, there exists no interpretation of GDPR considering the types of unique biometric data that can be derived from VR. Therefore, "how [the] GDPR would hold up against careful application of biometric psychography"—i.e., the commercial analysis and resale of VR-derived eye tracking data—remains uncertain.[175]

Having identified relevant gaps and uncertainties in the current regulatory framework, the concluding section of this note proposes a private-public partnership between federal legislators and the VR industry.

171. Commission Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 3 [hereinafter GDPR].

172. *Id.* at Art. 6(1)(a)–(f).

173. MCGILL, *supra* note 122, at 16.

174. Heller, *supra* note 64, at 43.

175. *Id.*

VI. PROPOSALS FOR REFORM: A PRIVATE-PUBLIC PARTNERSHIP

As VR technologies become more popular, developers and VR platforms will gain access to rich, new sources of information about individuals. This information is vulnerable to commercial exploitation due to gaps in the current U.S. regulatory framework; and, consequently, VR users are left exposed to a myriad of possible privacy harms. Policy solutions must toe a delicate line in addressing these concerns without stifling innovation and industry development. As the ITIF notes, "the approaches put in place today will impact how AR/VR devices and applications are developed for consumer, enterprise, and even government use well into the future."[176]

A. Background: Survey of Consumer Preferences Regarding Use of Eye Tracking Data in VR

Consumer preferences represent an intuitive starting point for considering policy-based solutions. One study from 2021 found a majority of VR users are uncomfortable with their biometric data being used to make inferences about them.[177] Specifically, 62% of respondents reported feeling uncomfortable with their biometric data being sold to advertisers and 57% felt the same for allowing it to be seen by law enforcement.[178] Only 35% of respondents reported discomfort with biometric data being used to further develop the product.[179]

One important takeaway is that "people don't like their data being used in ways in which they feel their control and autonomy is removed."[180] Accordingly, the authors conclude the study "provides evidence for and gives additional empirical research directions for the theory of contextual integrity developed by Helen Nissenbaum, which predicts that people's preferences would change based on data subject, sender, recipient, information type, and transmission principle."[181] In order to account for privacy's inherently contextual nature and honor consumer preferences, stakeholders and policy makers must "explore technical and policy choices that can shape social norms around XR and public trust in the technology."[182]

176. DICK, *supra* note 144, at 20.
177. Outlaw et al., *supra* note 119, at 15.
178. *Id.* at 16.
179. *Id.*
180. *Id.* at 25.
181. *Id.* at 27.
182. JEROME & GREENBERG, *supra* note 16, at 23.

B. Part 1: A Uniform Federal Privacy Framework

Professor Heller cautions that "extreme care should be taken when considering legislation," given that the "risk of derailing innovation is high" and eye tracking data is "particularly ripe for uncertainty and exploitation."[183] Accounting for these conflicting risks, this note supports the ITIF's proposal that, as an initial policy measure, Congress should establish a unified national privacy framework with preemptive force over existing state laws.[184] Importantly, the federal lawmakers should learn from the inapplicability of existing state laws' definitions of biometric information and explicitly clarify that any legislation covers biometric information *beyond purposes of identification*. Congressional lawmakers nearly made this mistake before: biometric privacy legislation introduced in 2019 sought to define "biometric identifier" almost identically to BIPA.[185] Federal legislation with statutory definitions going beyond identifiable or observable VR-derived data would both "encourage greater protection of this data and allow for a variety of use cases."[186]

Federal legislation should also establish a new regulatory authority for flexible and responsive oversight, which could serve as a bridge between policy makers and industry. Similar to FINRA, the self-regulatory organization created for the financial industry in 2017, federal law should mandate the creation of a comparable agency for the technology industry "to create ethical guidelines and craft (and enforce) regulation to better serve consumers."[187] While the ITIF has not expressly adopted this idea, it would effectively serve their goal to "better position regulators and developers alike

183. Heller, *supra* note 64, at 42.

184. *See* ALAN MCQUINN & DANIEL CASTRO, INFO. TECH. AND INNOVATION FOUND., A GRAND BARGAIN ON DATA PRIVACY LEGISLATION FOR AMERICA 2 (2019), https://www2.itif.org/2019-grand-bargain-privacy.pdf [https://perma.cc/7URE-FAP7]. Notably, Congressman Frank Pallone Jr. (D-NJ 6th District), Chairman of the House of Representatives Energy and Commerce Committee, introduced a federal data privacy bill on June 21, 2022. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022) (as introduced in the H. Comm. on Energy and Com., June 21, 2022). The law includes a much improved, comprehensive definition of biometric information that would cover "any . . . data generated from the technological processing of an individual's unique biological, physical, or physiological characteristics that is linked or reasonably linkable to an individual." The future of the bill has yet to be determined, but an amended version (with the same definition) was reported to the full house on December 30, 2022. *Id.* (as reported by the H. Comm. on Energy and Com., Dec. 30, 2022).

185. *See* National Biometric Information Privacy Act of 2020, S. 4400, 116th Cong. (2020).

186. DICK, *supra* note 144, at 21.

187. Hosfelt, *supra* note 131, at 7.

to ensure necessary safeguards are consistently implemented as [VR] technologies evolve."[188]

C. Part 2: VR Industry Self-Regulation

The VR industry itself should help mitigate the risks posed by its products. While corporate commitment to privacy and ethical principles are valuable, this note supports the concrete proposals put forth by the Future of Privacy Forum, who suggest that companies deploying immersive technologies should, at a minimum: (1) "establish clear policies regarding the collection, use, and sharing around sensitive XR data types, including user-provided location data and any biometrically-derived data"; (2) "limit third-party access to XR data and put in place procedures for responding to law enforcement or administrative demands for user information"; (3) "explore technical methods to automatically aggregate or pseudonymize XR data"; (4) "empower XR users through privacy protective default settings and easily accessible user controls"; and (5) "obtain prior user consent prior to conducting research *via* XR technologies."[189]

These measures would complement federal legislation by enabling not just ethical frameworks and guidance but, also, ethical practices. They could help establish "true informed consent" as the VR industry standard by requiring, in the words of Professor Heller, "a level of genuine understanding by the users about how their data is collected, applied, stored, and brokered."[190] These suggestions largely comport with the standards recommended by the ITIF as well.[191]

Voluntarily adopting these guidelines could serve a valuable reputational interest given that companies will want to establish themselves as leaders in the growing Metaverse industry. As commentators remarked back in 2018, "achieving recognition as both a cutting-edge and *responsible* [VR] developer may be a critical step in securing the consumer vote necessary to do so."[192]

188. DICK, *supra* note 144, at 22.

189. JEROME & GREENBERG, *supra* note 16, at 25–26. As an observation, Meta appears to satisfy a number of these requirements based off the Eye Tracking Privacy Policy accompanying its recently released Meta Quest Pro. *See Eye Tracking Privacy Policy*, *supra* note 87.

190. Heller, *supra* note 64, at 43.

191. *See* DICK, *supra* note 144, at 23.

192. Ed Klaris & Alexia Bedat, *Virtual Reality, Augmented Reality & Biometric Data After 2017*, KLARIS L. (Jan. 31, 2018), https://blog.klarislaw.com/vr-ar-virtual-reality-augmented-reality-biometric-data-after-2017-ed-klaris-alexia-bedat-a15e9cb000a1 [https://perma.cc/W3ZG-GWAY] (emphasis added).

CONCLUSION

"Privacy in VR has many utopian or dystopian outcomes, but it's likely to fall somewhere in between of being complicated and complex."[193] This note attempts to imagine that landing space, and ultimately proposes a multi-stakeholder arrangement based on transparency, consent, and practicality. When you look into the virtual world rendered by an HMD, you should know what the people who created that HMD are looking back at you.

193. Kent Bye, *Biometric Data Streams & the Unknown Ethical Threshold of Predicting & Controlling Behavior*, VOICES OF VR (Mar. 20, 2017), https://voicesofvr.com/517-biometric-data-streams-the-unknown-ethical-threshold-of-predicting-controlling-behavior/ [https://perma.cc/4SLK-PX5U].