Virtual Reality Data and Its Privacy Regulatory Challenges: A Call to Move Beyond Text-Based Informed Consent

Yeji Kim*

Oculus, a virtual reality company, recently announced that it will require all its users to have a personal Facebook account to access its full service. The announcement infuriated users around the world, who feared increased privacy risks from virtual reality, a computer-generated technology that creates a simulated world. The goal of virtual reality is to offer an immersive experience that appears as real as possible to its users. Providing such an experience necessitates collection, processing, and use of extensive user data, which begets corresponding privacy risks. But how extensive are the risks?

This Note examines the unique capacities and purpose of virtual reality and analyzes whether virtual reality data presents fundamentally greater privacy risks than data from other internet-connected devices, such as the Internet of Things (IoT), and if so, whether it poses any special challenges to data privacy regulation regimes, namely the European Union's General Data Protection Regulation (GDPR), the world's most stringent and influential data privacy law. Currently, one of the key criticisms of the GDPR is its low and ambiguous standard for obtaining users' "informed consent," or the process by which a fully informed user participates in decisions about their personal data. For example, a user who checks off a simple box after reading a privacy policy gives informed consent under the GDPR. This Note argues that virtual reality exposes a more fundamental problem of the GDPR: the futility of text-based informed consent in the context of virtual reality.

DOI: https://doi.org/10.15779/Z380Z70X6P.

[*] University of California, Berkeley, School of Law, Class of 2022.

I would like to thank Professor Paul Schwartz and the Samuelson Law, Technology & Public Policy Clinic for kindling my passion for privacy law. Special thanks to Professors Bertrall Ross and Joy Milligan, who have been incredible, encouraging mentors throughout the revision process. I am also so grateful to the California Law Review staff and Spring 2021 Note Publishing Workshop students for taking ownership on this Note and making the writing experience a communal one.

This Note supports this claim by analyzing how virtual reality widens the gap between the users' understanding of the implications of their consent and the actual implications. It first illustrates how virtual reality service providers must collect and process x-ray-like data from each user, such as physiological data like eye movements and gait, to provide customizations necessary to create an immersive experience. Based on this data, the service providers can know more about each user than what each user knows about themselves. Yet, this knowledge shift is not obvious to users. For virtual reality service to provide an immersive experience, customizations based on user data must be unnoticeable to users to avoid distractions. Using Oculus's recent privacy policy as a case study, this Note shows how this hidden knowledge shift transforms the meaning of ordinary privacy policy phrases like "an experience unique and relevant to you." What Oculus finds to be "relevant" to the user could be beyond what the user themselves would imagine to be "relevant." As a result, the text becomes an obsolete medium to communicate privacy risks to virtual reality users. This Note instead proposes other solutions—such as customizable privacy settings and visualization of privacy risks—for users to more closely understand and consciously weigh the benefits and the risks of using virtual reality.

INTRODUCTION

In August 2020, Oculus, a virtual reality company owned by Facebook, announced that it would require that all of its new users have a Facebook account.[1] Users with an existing Oculus account would need to merge that account with a Facebook account by 2023 to avoid losing the "full functionality" of their Oculus virtual reality headset.[2] This announcement infuriated many users around the world, who feared that linking their virtual reality activities to Facebook profiles would render them vulnerable to intrusive big data collection and processing.[3]

Big data refers to complex and large data sets—often from technological devices that collect and communicate data such as cell phones, health devices, and virtual reality—that businesses and organizations analyze to identify patterns in consumer behaviors and gather insights for business strategies.[4] Examples of virtual reality data include biometric data, like gait and eye movement, as well as behavioral data on how a user reacts to virtual challenges and tasks.[5]

Big data in general is already notoriously difficult to regulate. For example, many have discussed the fundamental tension between big data and consent-based regulatory models, such as the California Consumer Privacy Act (CCPA) and the GDPR.[6] Consent-based regulations presuppose that a user can make a well-informed decision about which data to share based on their knowledge of themselves, the data collected, and its possible risks.[7] Big data's key value, however, lies in its predictive analysis, which captures hidden meanings of data beyond human cognition.[8] Theoretically, this tension results in a catch-22: what big data can reveal is steps ahead of what a data subject can fathom about the consequences of their consent.

[1] *A Single Way to Log into Oculus and Unlock Social Features*, OCULUS BLOG (Aug. 18, 2020), https://www.oculus.com/blog/a-single-way-to-log-into-oculus-and-unlock-social-features/?locale=en_US [https://perma.cc/RXX6-WR3G].

[2] *Id.*

[3] *See* Adi Robertson, *Facebook Is Making Oculus' Worst Feature Unavoidable*, VERGE (Aug. 19, 2020), https://www.theverge.com/2020/8/19/21375118/oculus-facebook-account-login-data-privacy-controversy-developers-competition [https://perma.cc/8969-GJW2] ("The decision broke an early promise from Oculus founder Palmer Luckey . . . with critics raising concerns about intrusive data collection, targeted advertising, and being forced to use a service they hated.").

[4] *See* Nimrod Kaplan, *Big Data, Consumer Behavior and the Consumer Packaged Goods Blindspot*, FORBES (Sept. 5, 2019), https://www.forbes.com/sites/forbestechcouncil/2019/09/05/big-data-consumer-behavior-and-the-consumer-packaged-goods-blindspot/ [https://perma.cc/2B6D-CCVW].

[5] *See* Fiachra O'Brolcháin, Tim Jacquemard, David Monaghan, Noel O'Connor, Peter Novitzky & Bert Gordijn, *The Convergence of Virtual Reality and Social Networks: Threat to Privacy and Autonomy*, 22 SCI. & ENG'G ETHICS 1, 3–4 (2016); Pietro Cipresso, Irene Alice Chicchi Giglioli, Mariano Alcañiz Raya & Giuseppe Riva, *The Past, Present, and Future of Virtual and Augmented Reality Research: A Network and Cluster Analysis of the Literature*, 9 FRONTIERS PSYCH.1, 3 (2018).

[6] *See, e.g.*, Tal Z. Zarsky, *Incompatible: The GDPR in the Age of Big Data*, 47 SETON HALL L. REV. 995, 1002–04 (2017); *see also* Rainer Lenz, *Big Data: Ethics and Law* 20–28 (Collaboration in Higher Educ. for Digit. Transformation in European Bus., Working Paper, 2019), https://www.chedteb.eu/media/attachments/2019/09/18/big-data---ethics-and-law.pdf [https://perma.cc/8WJD-9WNW].

[7] *See* Lenz, *supra* note 6, at 21.

[8] *See id.* at 4.

Given big data's known privacy risks and regulatory challenges, this Note examines: (1) whether the data processed[9] from virtual reality is in fact different from other big data, and if so, (2) whether this difference poses any special challenges for the consent-based regulatory models, namely the GDPR. Since it took effect in 2018, the GDPR has been considered the gold standard for data privacy, as it imposes the strictest data privacy regulations in the world.[10] Although enacted by the European Union, it imposes data-related obligations on any organization that "target[s] or collect[s] data" related to people in the European Union.[11] This means that the GDPR has a jurisdiction to regulate how U.S. companies like Oculus and Facebook collect and process data. The GDPR has also influenced many countries' data privacy laws, including U.S. state laws, such as the CCPA. For example, the CCPA drew its provisions from many of the GDPR's key principles and languages, such as an "individual's right to know" about the data collected about them and a right to "opt out" of approving an organization to sell their personal information to third parties.[12]

Although the United States has yet to enact a federal statute on data privacy, many have expressed the increasing need to do so and are hopeful about its passage in the next few years.[13] Understanding the shortcomings of the GDPR would help guide a potential U.S. federal statute or state privacy statute to minimize privacy risks while promoting innovation. Despite its title as the world's most stringent data privacy law, the GDPR has its shortcomings in regulating data. One important criticism is on the requirement of users' informed consent, which refers to "the process by which a fully informed user participates in decisions about [their] personal data."[14] For example, many have criticized the GDPR's standard of informed consent for being too low, because it involves simply checking a box without requiring the users to read the privacy policies.[15]

[9] Here, I use the term "processing" as a term of art, as defined by GDPR Article 4(2): "'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction." Regulation 2016/679 of the European Parliament and of the Council of Apr. 27, 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), art. 4(2), 2016 OJ (L 119) 33 (EU) [hereinafter GDPR].

[10] *See What Is GDPR, the EU's New Data Protection Law?*, GDPR.EU (Feb. 13, 2019), https://gdpr.eu/what-is-gdpr/ [https://perma.cc/RD8V-SHMR].

[11] *Id.*

[12] Paul Schwartz, *Global Data Privacy: The EU Way*, 94 N.Y.U. L. REV. 771, 817 (2019).

[13] *See* Jennifer Bryant, *2021 'Best Chance' for US Privacy Legislation*, IAPP (Dec. 7, 2020), https://iapp.org/news/a/2021-best-chance-for-federal-privacy-legislation/ [https://perma.cc/TGT2-7C7T].

[14] Masooda Bashir, Carol Hayes, April D. Lambert & Jay P. Kesan, *Online Privacy and Informed Consent: The Dilemma of Information Asymmetry*, 52 PROC. ASS'N INFO. SCI. & TECH. 1, 3 (2016).

[15] *See, e.g.*, Lorena Barrenechea Salazar, *Privacy, the Fallacy of Consent and the Need to Regulate Social Media Platforms*, 1 INTERGOVERNMENTAL ORGS. IN-HOUSE COUNS. J. 39 (2020).

Others have discussed the ambiguity of what constitutes informed consent in the context of virtual reality data processing.[16] These criticisms suggest that raising or clarifying the informed consent standard would help solve the current regulatory challenges.[17]

This Note seeks to contribute to the discussion of the GDPR's regulation of virtual reality data by identifying a more fundamental problem: the futility of text-based informed consent in the context of virtual reality. This Note claims that the unique capacities of virtual reality data exacerbate the gap between users' understanding of their consent and the actual implications of the consent—to the point that obtaining a user's informed consent following the reading of a text-based privacy policy becomes a hollow ideal. Raising or clarifying the standard of informed consent is also not enough to address virtual reality regulatory challenges. Instead, we need to move away from text-based informed consent and reimagine the means to protect the privacy rights of data subjects.

Specifically, this Note strives to show how traditional forms of obtaining informed consent are futile in virtual reality. First, this Note illustrates how virtual reality debunks a premise of informed consent: that users themselves are best positioned to discern what constitutes their unique private information and therefore properly control which information to grant and deny access.[18] A virtual reality headset can collect an unprecedented wealth of x-ray-like data about each user, such as physiological and psychological traits, that allows a virtual reality service provider to know each user more intimately than the user may know themselves. This knowledge shift debunks a premise of informed consent in data collection and processing—that the user, as opposed to service providers, knows what constitutes their private information.

Yet, this knowledge shift is not obvious to users. For example, virtual reality allows companies to provide sophisticated and unnoticeable personalization to users.[19] Companies identify, respond to, and shape the user's

[16] *See, e.g.*, Emil Albihn Henriksson, *Data Protection Challenges for Virtual Reality Applications*, 1 INTERACTIVE ENT. L. REV. 57, 60 (2018) ("[C]onsent might not be considered as freely given if the provision of a service is conditional on consent to the processing of personal data that is not necessary for the performance of that service . . . . [T]here might be a question of where that line is drawn. Is game telemetry for instance necessary for the provision of a game? Arguably this collection is part and parcel of providing the game but the opposite stance cannot be ruled out.").

[17] *See id.*

[18] *See* Stuart S. Shapiro, Travis D. Breaux & David Gordon, *Engineering and Privacy*, *in* AN INTRODUCTION TO PRIVACY FOR TECHNOLOGY PROFESSIONALS 28 (Travis D. Breaux ed., 2020) ("One approach is to transfer control to the individual whenever possible to allow them to manage their own privacy risks. While this approach requires designing systems to expose this level of control to users, the underlying premise is that individuals know their unique privacy risks better than outsiders, whereas IT professionals may misjudge the risk or be unfamiliar with the individual's personal circumstances.").

[19] Bartłomiej Pierański & Sergiusz Strykowski, *Towards a Personalized Virtual Customer Experience*, *in* 710 STUDIES IN COMPUTATIONAL INTELLIGENCE 185, 190 (Dariusz Król et al. eds. 2017) (describing how ambient elements influence consumers on a more subconscious level and how virtual reality allows companies to design atmospheric elements, such as visual and aural, with ease).

subconscious needs in real-time—such as the optimal level of visual, auditory, and textile background for that user—to induce the user to purchase products on virtual reality without being aware of the influence from the personalization.[20] While other internet-connected devices also provide subtle personalized services, virtual reality, by definition, must strive for the personalization to be unrecognized. The goal of virtual reality is to provide an immersive experience as real as possible; noticeable personalization distracts users from being fully immersed.

Then, this Note analyzes the consequences of this knowledge shift. This Note's secondary contribution is to show how these unique capacities of virtual reality would unfathomably transform the meanings of ordinary privacy policy phrases like "unique and relevant to you" that define the scope of data processing in privacy policies. What a virtual reality service provider finds to be "relevant" to the user based on the data it has about the user could be beyond the grasp of what the user would imagine to be relevant—such as the optimal amount of visual or aural effects personalized to the user that induce them to purchase a product on virtual reality.[21] As a result, text becomes an even more imperfect medium to communicate to the users about their privacy risks. Despite this gap in users' expectations, virtual reality data processing does not violate the GDPR—at least not blatantly. This is problematic because such processing undermines data subjects' right to information self-determination, a tenet of the GDPR.

This Note consists of four parts. Part I explains the characteristics of big data in general and problems in regulating big data. Part II analyzes how the data processed from virtual reality is different from other existing big data. Part III analyzes Oculus's most recent Privacy Policy, effective October 11, 2020, and evaluates how it may comply with the GDPR, despite the fact that its language cannot adequately communicate the scope of data processing to its users.[22] Oculus's Privacy Policy is a helpful case study for two reasons. First, Oculus overhauled its most recent policy after announcing the requirement to use a Facebook account for all users; subsequent updates, unless the United States passes a federal statute, would likely be minor. Second, because the policy is written in clear and concise language, it ironically showcases how the collection

[20] *See id.* at 190–91.

[21] *Id.* ("All the ambient elements can influence shoppers within a range that is limited by two elements: stimulus awareness and stimulus overload. If the intensity of an ambient element (lighting level, music volume, etc.) is too low (lower than the level of stimulus awareness) shoppers will not be affected by them. On the other hand, however, if the intensity is higher than the stimulus overload point shoppers will experience perceptual overloading . . . . It is not surprising that for each customer the level of acceptable intensity, as well as the level of stimulus awareness and overload, can be different . . . . VR makes it possible to personalize each of the above mentioned ambient elements.").

[22] Although effective starting October 11, 2020, Oculus published the new Policy on an earlier date. For the most recent version, see *Oculus Privacy Policy*, OCULUS (Oct. 11, 2020), https://www.oculus.com/legal/privacy-policy-for-oculus-account-users/ [https://perma.cc/LAM6-3ZTR].

and processing of virtual reality data transform ordinary privacy policy languages in ways unfathomable to users. Part IV proposes solutions, such as customized virtual reality settings and visualization of privacy risks, to reimagine the means to protect the data privacy rights of the virtual reality users.

I.
BIG DATA AND ITS REGULATORY CHALLENGES

Big data refers to complex and large data sets, which must be analyzed to uncover actionable insights for businesses and organizations.[23] It is typically characterized by four V's: volume, variety, veracity, and velocity.[24]

Volume refers to the size of big data, which is often so big as to require a multitiered storage media.[25] Most U.S. companies today have at least one-hundred terabytes, or one hundred thousand gigabytes, of data stored.[26]

Variety means that the data is collected from multiple sources and forms. Broadly speaking, three forms of data exist: structured, unstructured, and semi-structured. Structured refers to data organized into predefined fields, like spreadsheets, which are easy to search and analyze.[27] Unstructured data is complex and does not fit into a predefined organization.[28] It includes a wide array of formats, such as social media postings and YouTube videos.[29] About 80 percent of big data is unstructured,[30] which means that most of big data require sophisticated analytic tools to make sense of the vast mine of data waiting to be cultivated. It also means that the external context of the unstructured data helps to imbue meaning to the data.[31] For example, analyzing a log of YouTube videos

[23] *See* Svetlana Sicular, *Gartner's Big Data Definition Consists of Three Parts, Not to Be Confused with Three "V"s*, FORBES (Mar. 27, 2013), https://www.forbes.com/sites/gartnergroup/2013/03/27/gartners-big-data-definition-consists-of-three-parts-not-to-be-confused-with-three-vs/#710058542f68 [https://perma.cc/5PL5-564Y].

[24] Some experts use 3 V's definition, which omits "veracity." This paper adopted a 4 V's definition, because "veracity" constitutes an important characteristic of virtual reality data. For a 3 V's version of the definition, see *id.* For why veracity is an important characteristic of big data, see Seth Grimes, *4 Vs for Big Data Analytics*, BREAKTHROUGH ANALYSIS (July 31, 2013), http://breakthroughanalysis.com/2013/07/31/4-vs-for-big-data-analytics/ [https://perma.cc/4P3W-DPRD].

[25] Leighton Johnson, *4 Vs of Big Data*, ISACA (June 12, 2019), https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2019/volume-12/4-vs-of-big-data [https://perma.cc/79X9-MZZC].

[26] IBM, THE FOUR V'S OF BIG DATA (2013), https://www.ibmbigdatahub.com/infographic/four-vs-big-data [https://perma.cc/K97S-QG2Z].

[27] *See* Christine Taylor, *Structured vs. Unstructured Data*, DATAMATION (Mar. 28, 2018), https://www.datamation.com/big-data/structured-vs-unstructured-data.html [https://perma.cc/44C5-SCRC].

[28] *See id.*

[29] *Id.*

[30] *See* Richard Allen, *What Are the Types of Big Data?*, SELECTHUB (July 13, 2021), https://www.selecthub.com/big-data-analytics/types-of-big-data-analytics/ [https://perma.cc/92JH-D2XG] ("The consensus is no more than 20% of all data is structured.").

[31] *See id.* ("[C]ontext is almost, if not as, important as the information wrung out of the data. . . . [A] query on an unstructured data set might yield the number 31, but without context it's meaningless.

streamed would become easier and result in more sophisticated insights if accompanied by demographics information and the time of the day.[32]

The next element of the four V's is veracity, which refers to both the quality of data and its processing.[33] Quality of data refers to its reliability and accuracy—more reliable data is relatively free of bias, inconsistency, and volatility.[34] An example of a highly reliable data is a medical experiment or a trial that follows strict procedures for the control group.[35]

The final element, velocity, refers to the speed at which the data is analyzed. This includes the speed of inputs, such as processing social media posts, and outputs, such as the processing required to create a report analyzing those posts.[36] For example, the New York Stock Exchange processes one trilobite of trade information during each trading session.[37]

The advantage of big data lies in predictive analysis: giving businesses and organizations actionable insights to make better decisions. Big data excavates patterns and meanings hidden from the human eye. For example, big data analysis can predict who would have Parkinson's disease based on analyzing subtle mouse tremors when clicking on website information.[38] This information could be applied in many areas, ranging from health professionals providing tailored medical services to marketers targeting specific individuals. Because big data is like a gold mine yet to be explored, it is already a huge asset in the digital economy.[39] The top five sources of big data include media, cloud, web, and IoT devices and databases.[40] Media data analysis provides insights on consumer preferences and changing trends.[41] IoT, which includes medical devices, video

It could be 'the number of days in a month, the amount of dollars a stock increased . . . , or the number of items sold today.' . . . The contextual aspect is what makes unstructured data ubiquitous in big data: merging internal data with external context makes it more meaningful.").

[32] *See* Christina Newberry & Katie Sehl, *YouTube Analytics: How to Use Data to Grow Your Channel Faster*, HOOTSUITE (July 28, 2021), https://blog.hootsuite.com/youtube-analytics/ [https://perma.cc/DGZ8-KUHJ] (noting how YouTube video metrics data, such as audience demographics, traffic sources, and keywords, would bring actionable insights to refine marketing and content strategies of YouTube channels).

[33] *Veracity: The Most Important "V" of Big Data*, GUTCHECK (Aug. 29, 2019), https://www.gutcheckit.com/blog/veracity-big-data-v/ [https://perma.cc/M3VV-WA5A].

[34] *Id.*

[35] *The Four V's of Big Data: The 4 Characteristics of Big Data*, ENTERPRISE BIG DATA FRAMEWORK (Oct. 16, 2020), https://www.bigdataframework.org/four-vs-of-big-data/ [https://perma.cc/2RJ7-25XS].

[36] *See* John Spacey, *5 Types of Data Velocity*, SIMPLICABLE (Nov. 29, 2017), https://simplicable.com/new/data-velocity [https://perma.cc/GH8T-MTQE].

[37] IBM, *supra* note 26.

[38] *See generally* Ryen W. White, P. Murali Doraiswamy & Eric Horvitz, *Detecting Neurodegenerative Disorders from Web Search Signals*, 1 NPJ DIGIT. MED., no. 8, 2018.

[39] *See* Taylor, *supra* note 27 (discussing the differences between structured and unstructured data and explaining how "[u]nstructured data analytics with machine-learning intelligence" can allow organizations to, among other things, "[g]ain new marketing intelligence").

[40] Naveen Joshi, *Top 5 Sources of Big Data*, ALLERIN (Nov. 26, 2017), https://www.allerin.com/blog/top-5-sources-of-big-data [https://perma.cc/JFN3-H3XZ].

[41] *Id.*

games, vehicular processes, and cameras, is gaining traction.[42] For example, a medical device collects real-time glucose insights for patients with diabetes, and uses the data points to analyze the connection between glucose levels, medication, and lifestyle choices.[43]

Because big data's processing can reveal intimate information about individuals, many have criticized today's consent-based regulatory frameworks, such as the GDPR, as making faulty assumptions about big data.[44] The current regulatory frameworks categorize types of data—such as personal data, sensitive data, non-identifying information—prior to its processing and require ex-ante consent to the processing.[45] However, the data initially collected can change its nature over time as companies process that data.[46] Non-sensitive data may be combined with other non-sensitive data to generate sensitive data. Moreover, even if not combined with other data, a set of data repeats the process of being anonymized and de-anonymized, depending on the purpose of the data analysis and use.[47] Thus, the ex-ante consent and ex-post data regulatory analysis creates a gap between the data subject's understanding of their consent and the actual consequences of their consent.

II.
VIRTUAL REALITY: EXAMINED THROUGH THREE V'S OF BIG DATA

For years, the advent of virtual reality has excited people across many different areas, such as education, healthcare, architecture, and even legal enforcement.[48] The key defining feature of virtual reality is the experience of mental and spatial "presence" in a different world, ideally a presence so real that a user would perceive and behave as they would in the real world.[49] The potential applications of this technology are limitless. Although virtual reality tech is primarily used for gaming as of now, some predict that it will impact anything

[42] *Id.*

[43] *See Big Data Predictive Analytics: The Future of Medical Devices*, MED. DEVICE NETWORK (Nov. 30, 2018), https://www.medicaldevice-network.com/comment/medical-device-industry-growth/ [https://perma.cc/N2R6-K8VH].

[44] *See* Lenz, *supra* note 6, at 21.

[45] *See* GDPR, *supra* note 9, art. 9.

[46] Lenz, *supra* note 6, at 22.

[47] *See* Bart van der Sloot & Sascha van Schendel, *Ten Questions for Future Regulation of Big Data: A Comparative and Empirical Legal Study*, 7 J. INTELL. PROP. INFO. TECH. & ELEC. COM. L. 110, 124 (2016).

[48] *See* Sophie Thompson, *VR Applications: 21 Industries Already Using Virtual Reality*, VIRTUALSPEECH (Dec. 11, 2020), https://virtualspeech.com/blog/vr-applications [https://perma.cc/L7RE-3F9L].

[49] *See* Devon Adams, Alseny Bah, Catherine Barwulor, Nureli Musaby, Kadeem Pitkin & Elissa M. Redmiles, *Ethics Emerging: The Story of Privacy and Security Perceptions in Virtual Reality*, *in* PROCEEDINGS OF THE FOURTEENTH SYMPOSIUM ON USABLE PRIVACY AND SECURITY 443, 448 (2018) ("[T]he majority of developers . . . mentioned that their primary goal was to facilitate and ensure a sense of 'presence.'").

that has a "spatial component" in the commercial sector.[50] For example, workplaces are already introducing virtual reality for safety training simulation.[51] Mark Zuckerberg stated that virtual reality "could change the future of social media interaction."[52]

Virtual reality data—given its large volume and varied types of data that must be processed to create an immersive experience—is a form of big data. At the same time, it exacerbates the gap in user expectations more than other preexisting big data does, such as ones from web and health devices. To show how virtual reality data poses different challenges from other big data, this Section analyzes the characteristics of virtual reality data in terms of three V's of big data: variety, veracity, and velocity. This Note omits analysis for the "volume" element of the four V's. Although increases in volume may render virtual reality data more vulnerable to cybersecurity breaches, cybersecurity is not the focus of this Note.

This Note argues that data processed from virtual reality exacerbates the tension between big data and the GDPR in each of the three dimensions of big data—variety, veracity, and velocity. First, variety: virtual reality collects unprecedentedly in-depth and varied kinds of data, which may not reveal the users' identity in individual data sets but which can do so when varied data sets are taken in aggregate. This development exacerbates the already eroding boundary between identifying and non-identifying personal information. Second, veracity: virtual reality presents an enticing venue for scientific experiments, but this venue is fundamentally flawed because data subjects' behaviors in virtual reality can deviate from their real behaviors. Yet, such data can be used to profile and penalize users. Third, velocity: real-time processing of data in virtual reality could enable even more subtle forms of psychological persuasion of its users than is possible with other forms of big data.

A. "Variety" of Virtual Reality Data: Self-Sufficing Ecosystem

Virtual reality is different from other digital realities, such as augmented or mixed reality, in that it aims to provide the experience of immersion, where the real world completely disappears from the user and the user is absorbed in a

[50] Michel Martin, *Take a Peek Under the Helmet of Virtual Reality at SXSW*, NPR (Mar. 19, 2017), http://www.npr.org/2017/03/19/520752758/take-a-peek-underthe-helmet-of-virtual-reality-at-south-by-southwest [https://perma.cc/N26D-5AB6].

[51] *See, e.g.*, Maria Korolov, *The Real Risks of Virtual Reality*, RISK MGMT. MAG. (Oct. 1, 2014), http://www.rmmagazine.com/2014/10/01/the-real-risks-of-virtual-reality/ [https://perma.cc/QV5Y-TE8P] ("[E]ven though the Oculus Rift and similar devices have not hit the market yet, companies are already using virtual reality for training, simulations, manufacturing prototypes and marketing. Insurer Travelers, for example, has developed a virtual warehouse using the Oculus Rift to teach workplace safety strategies.").

[52] Crystal Nwaneri, *Ready Lawyer One: Legal Issues in the Innovation of Virtual Reality*, 30 HARV. J.L. & TECH. 601, 606 (2017).

different world.[53] Immersion also means that the user is not only present in the different world but also interacts with it and affects changes. For example, they can pick up a virtual object, throw it, and engage with people within the virtual reality.[54]

Data collected from virtual reality can be divided into two categories. First, virtual reality collects many kinds of physiological data needed to create an immersive experience for their users.[55] For instance, as a user moves and changes their body position, the user's viewing angles to the virtual reality scene must change as well, just like in the real world.[56] In order to accomplish this responsiveness, virtual reality headsets have motion detector sensors attached; the sensors detect the user's body position in space and even provide haptic, or touch, feedback.[57] They also collect biometrically-derived data about one's gaze, gait, and head and body movement.[58] For example, hand tracking—which allows users to manipulate virtual objects—is becoming a standard feature.[59]

Second, virtual reality collects data on how the users behave in an immersive virtual world, such as how they interact with other users and perform game tasks.[60] In short, virtual reality collects comprehensive information on how the user's body and mind respond to virtual stimuli.

[53] *See* Patrick Hehn, Dariah Lutsch & Frank Pessel, *Inducing Context with Immersive Technologies in Sensory Consumer Testing*, *in* CONTEXT: THE EFFECTS OF ENVIRONMENT ON PRODUCT DESIGN AND EVALUATION 475, 476 (Herbert L. Meiselman ed., 2019) ("Everything in between can be called mixed or merged reality. The real environment disappears completely in the virtual environment (virtual reality) while in augmented reality, the portion of the real environment predominates.").

[54] *See, e.g.*, Kel Smith, *Virtual Reality, Universal Life*, *in* DIGITAL OUTCASTS: MOVING TECHNOLOGY FORWARD WITHOUT LEAVING PEOPLE BEHIND 157, 166 (2013) ("Haptic devices offer players the ability to hold and pick up virtual objects, with an effect realistic enough to simulate weight and texture."); *id.* at 179 ("For people who suddenly become sequestered from their community of support, virtual worlds provide an immediacy and presence that other digital vehicles (such as email) simply cannot match. What participants discover is that the community has found and welcomed them, offering a shared space that is powerfully compelling.").

[55] *See* Cipresso et al., *supra* note 5, at 3 (describing technologies, such as "tracking devices as bend-sending gloves that detect the fingers movements, postures and gestures, or pinch gloves that detect the fingers movements, and trackers able to follow the user's movements in the physical world and translate them in the virtual environment").

[56] *See id.* at 2 (explaining that virtual reality creates an immersive experience by using sensory devices such as head mounted displays (HMDs) that enhance a user's view of the virtual environment by capturing the user's head movement).

[57] *See* O'Brolcháin et al., *supra* note 5, at 3–4; Cipresso et al., *supra* note 5, at 3.

[58] *See* Cipresso et al., *supra* note 5, at 2 (describing that "VR relies on a 3D, stereoscopic head-tracker displays, hand/body tracking and binaural sound").

[59] *See Oculus Touch Launches Today!*, OCULUS BLOG (Dec. 6, 2016), https://www.oculus.com/blog/oculus-touch-launches-today/ [https://perma.cc/3XWD-TMCN].

[60] *See* Cipresso et al., *supra* note 5, at 2 ("Currently, videogames supported by VR tools are more popular than the past, and they represent valuables, work-related tools for neuroscientists, psychologists, biologists, and other researchers as well. Indeed, for example, one of the main research purposes lies from navigation studies that include complex experiments that could be done in a laboratory by using VR, whereas, without VR, the researchers would have to go directly into the field, possibly with limited use of intervention.").

This x-ray-like data gathered from virtual reality redefines the meaning of "variety" in big data. Although the data comes in varied forms, it is still orderly, amenable to aggregate analysis. Previously, the term "variety" accentuated the unordered, messy nature of multiple forms of data, which are not readily integrated or processed.[61] For example, understanding the meaning of a phone log is difficult, because the external context of such calls—such as the person's mood at the time—may not be readily accessible.

Thus, companies had to engage in data trading to supplement their internally-collected data with data that provides external context to derive a meaningful analysis.[62] Companies engage in data trading by first identifying who has the data the company needs, negotiating the value of the data, and drafting an agreement.[63] Yet, data trading poses many hurdles. Because data is considered proprietary, many companies are reluctant to trade their data.[64] Even if they do decide to trade, companies need to ensure that such trading would comply with data transfer regulations.[65]

Given these hurdles in data trading, the advantage of virtual reality data is that the data processed is so extensive that the virtual reality providers would have less need to engage in data trading. This is because virtual reality operates as its own closed world: what is considered a typical "external" context is happening internally in virtual reality. For example, the context of each person's movement, such as a task at hand or interaction with others, is collected with other physiological information.[66] This immersive nature of virtual reality allows it to collect its own self-sufficing ecosystem of data, where the data can be analyzed without needing additional context.

The fact that virtual reality providers do not need to engage in data trading enables easier data analysis and expands the scope of possible inferences, which muddies the boundary between identifying and non-identifying personal information. Individually, the data collected from virtual reality is not any more revealing compared to big data from other platforms, such as various health monitoring devices like Fitbit that track and monitor our heart rate and sleeping

[61] *See* Edd Dumbill, *Volume, Velocity, Variety: What You Need to Know About Big Data*, FORBES (Jan. 19, 2012), https://www.forbes.com/sites/oreillymedia/2012/01/19/volume-velocity-variety-what-you-need-to-know-about-big-data/#520b0c171b6d [https://perma.cc/JVD4-TVVH].

[62] *See* George Bailey, *The Key to Unlocking the Power of AI: Data Trading*, FORBES (Mar. 31, 2019), https://www.forbes.com/sites/georgebailey1/2019/03/31/the-key-to-unlocking-the-power-of-ai-data-trading/#33ee86a03bf2 [https://perma.cc/S9TH-2DGQ].

[63] *See id.*

[64] *Id.* ("Based on our interviews with business leaders, most companies are frustrated by the lack of data sharing with their customers and suppliers. Of course, one issue is the desire to protect proprietary data and not lose a competitive advantage.").

[65] *See, e.g.*, GDPR, *supra* note 9, art. 44.

[66] *See* 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=2588e66b3459 [https://perma.cc/68TC-XHXN] (explaining how tracking a virtual reality user's eye movements would measure how a user reacts to what they are seeing, thereby drawing powerful actionable marketing insights).

patterns.[67] However, the physiological and behavioral data from virtual reality—as an aggregate—can form a "kinematic fingerprint," identifying an individual just as a fingerprint would.[68] For example, movement of a joint alone cannot identify an individual, but a collection of body movements, of "how one moves, coordinates and uses body segments in relation to each other[,]" can identify an individual at 60 percent accuracy rate.[69]

B. "Veracity" of Virtual Reality Data: Reliable at the Expense of Some

Although virtual reality data processing can reveal insightful information about each user, the data may be fundamentally flawed. On the one hand, virtual reality provides a perfect venue for experiments. Engineers create virtual reality, aiming to simulate a world for users to engage in "targeted behavior,"[70] for entertainment, such as flying, walking, and exploring. To induce users to fly, engineers can program the same repeated sequence for all participants, such as the course of flying, obstacles faced, and duration.[71] Virtual reality operates as a controlled, lab-like world, where the world itself functions as an independent variable and the users as experiment subjects or dependent variables. This kind of experiment—on how users physically, psychologically, and behaviorally respond to the task in virtual reality—allows data analysists to draw insights and inferences about users' responses in general and about each individual's tendencies.[72] Researchers are already taking advantage of virtual reality to run experiments. For example, a medical research team experimented to identify children with Autism Spectrum Disorder by having the subjects participate in virtual reality activities and analyzing the children's body movements.[73] The team simulated a city-street interaction—that "identically repeated three times"—for each of the children.[74] The participants were instructed to imitate an

[67] *See Mobile Devices Driving Unprecedented Growth in Self-Monitoring Technologies Markets, According to BCC Research*, BCC RSCH. (June 29, 2015), https://www.bccresearch.com/pressroom/hlc/mobile-devices-driving-unprecedented-growth-in-self-monitoring-technologies-markets [https://perma.cc/H3RF-AYT2].

[68] Michael Madary & Thomas K. Metzinger, *Real Virtuality: A Code of Ethical Conduct. Recommendations for Good Scientific Practice and the Consumers of VR-Technology*, 3 FRONTIERS ROBOTICS & AI, no. 3, 2016, at 1, 12.

[69] Specifically, the study had a 63.55 percent accuracy rate in identifying the individual by having them point at a target; 49.67 percent for walking. Ken Pfeuffer, Matthias J. Geiger, Sarah Prange, Lukas Mecke, Daniel Buschek & Florian Alt, *Behavioural Biometrics in VR: Identifying People from Body Motion and Relations in Virtual Reality*, *in* CHI 2019: PROCEEDINGS OF THE 2019 CHI CONFERENCE ON HUMAN FACTORS IN COMPUTER SYSTEMS, Paper no. 110, at 9 (2019).

[70] Hehn et al., *supra* note 53, at 475.

[71] *See, e.g.*, Mariano Alcañiz Raya, Javier Marin-Morales, Maria Eleonora Minissi, Gonzalo Teruel Garcia, Luis Abad & Irene Alice Chicchi Giglioli, *Machine Learning and Virtual Reality on Body Movements' Behaviors to Classify Children with Autism Spectrum Disorder*, 9 J. CLINICAL MED., no. 1260, May 2020, at 6 (explaining how the research team developed the experiment by using identical VR program sequence for each child).

[72] *See id.*

[73] *Id.* at 5.

[74] *Id.* at 6.

avatar's actions, such as disco dancing.[75] By analyzing children's joint movements, the research team found that autistic children presented larger body movements than neurotypical children, identifying autistic children with an 80 percent or higher success rate.[76]

Although virtual reality may provide a perfect *procedural* ground for experiments, users in virtual reality may also behave differently from how they would in real life. "Virtual" in the virtual reality means "almost"—almost, but not quite the actual reality.[77] Virtual reality provides an immersive experience by "manipulating perception via false sensory cues."[78] A team at Oxford recently conducted research on how real the dangers in virtual reality feel to its participants.[79] When told to jump off the virtual cliff, the participants felt "real physical fear, sweaty palms, and a racing heart."[80] Only one in ten mustered the courage to jump off the cliff; those who did felt a "sensation akin to physical pain."[81] Although the experiment shows how closely virtual reality can mimic experiences in real life, no one in real life—if told to jump off the deadly cliff—would do so if they had the will to continue living. The fact that one in ten managed to jump off the virtual cliff indicates that some people's behavior would differ in real life. This behavioral deviation is also demonstrated in other research, which showcases those who do not vote in real life are politically active in virtual reality.[82] The level of deviation is likely also context-dependent, which poses a challenge in even identifying the kind of person who would behave differently in a particular situation.

Therefore, virtual reality data analysis could be both highly accurate thanks to its lab-like environment and highly inaccurate regarding some people whose behavior deviates in virtual reality. The latter group could be harmed by having inaccurate inferences drawn about them. An example of such harm could be a potential reduction in employment prospects. A candidate could be harmed if an employer chooses not to hire them because of an incorrect behavioral inference drawn about them based on how they behave in the virtual world.[83]

[75] *Id.* at 6–7.

[76] *Id.* at 13.

[77] William Safire, *ON LANGUAGE; Virtual Reality*, N.Y. TIMES (Sept. 13, 1992), https://www.nytimes.com/1992/09/13/magazine/on-language-virtual-reality.html? [https://perma.cc/D9W5-9BYD].

[78] Gilad Yadin, *Virtual Reality Surveillance*, 35 CARDOZO ARTS & ENT. L.J. 707, 726 (2017).

[79] *See id.* at 728.

[80] *Id.*

[81] *Id.*

[82] *See* Sherry Turkle, *Virtual Reality, Psychology of*, INT'L ENCYC. SOC. & BEHAV. SCI. 16214, 16217 (2001).

[83] *See, e.g.*, *How to Use Virtual Reality and AI in Recruitment: Part 2*, VIRTI (July 16, 2021), https://insights.virti.com/how-to-use-virtual-reality-and-ai-in-recruitment-part-2/ [https://perma.cc/42FQ-5JQA] (describing how virtual reality can transform the hiring process by examining how candidates navigate a virtual environment and interact with digitized customers and evaluating candidates' ability to synthesize information).

Moreover, even if virtual reality data inferences are accurate, the depth and breadth of possible inferences about individuals aggravate the problem of "penalty based on propensity," or profiling people based on what big data suggests that they are likely to do or develop.[84]

C. *"Velocity" of Virtual Reality Data: Real-Time Processing*

Another distinguishing feature of virtual reality data is its high velocity, or the speed at which the data is analyzed. To provide a seamless immersive experience, virtual reality providers must process certain data, such as body movement, in real time, so that the users' avatars can accurately reflect the users' current physiological manifestations. Virtual reality service providers will soon be able to customize the users' experience based on real-time understanding of each user's emotional and physiological state.[85] This real-time interaction between data processing and users enables new techniques of subtle psychological persuasions.

One value of big data is its analytic power to psychologically persuade people. A Chief Data Scientist of a Silicon Valley company said that the goal of big data predictive analysis is "to change people's actual behavior at scale . . . . We can capture their behaviors, identify good and bad behaviors, and develop ways to reward the good and punish the bad."[86] A research study has already shown that social networks such as Facebook can create a massive-scale emotional contagion.[87] For example, when a research study reduced positive words in Facebook's news feeds, the users viewing the news feeds posted status updates with fewer positive words and more negative words.[88] Emotions can be transferred to others, and people can "experience the same emotions without their awareness."[89] Psychological targeting in a social media platform is becoming an effective instrument for digital mass persuasion as a way to influence voters and consumers.[90]

[84] *See* Shitong Cao & Ajay K. Manrai, *Big Data in Marketing & Retailing*, 1 J. INT'L & INTERDISC. BUS. RSCH. 23, 28–29 (2014).

[85] *See, e.g.*, Lee Roth, *How IoT Can Improve the Shopper's Experience*, CLARITY CONSULTING BLOG (Jan. 20, 2017), https://blogs.claritycon.com/how-iot-can-improve-the-shoppers-experience-e54a538d0e7e [https://perma.cc/9ZNW-M3Q8] (describing a smart shelf that changes its display based on shopper "linger time," demographics, and visual focus).

[86] Bruce Sterling, *Shoshanna Zuboff Condemning Google "Surveillance Capitalism*,*"* WIRED (Mar. 8, 2016), https://www.wired.com/beyond-the-beyond/2016/03/shoshanna-zuboff-condemning-google-surveillance-capitalism/ [https://perma.cc/MWM9-TQWB].

[87] *See* Adam D. I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PROC. NAT'L ACAD. SCI. 8788 (2014).

[88] *Id.* at 8788.

[89] *Id.*

[90] *See* Edmund L. Andrews, *The Science Behind Cambridge Analytica: Does Psychological Profiling Work?*, INSIGHTS STAN. BUS. (Apr. 12, 2018), https://www.gsb.stanford.edu/insights/science-behind-cambridge-analytica-does-psychological-profiling-work [https://perma.cc/58ZM-VQLC].

Virtual reality's real-time processing of data overcomes two current limitations in psychologically persuading people. The first limitation is that the psychological meaning of certain digital footprints and its relationship to specific psychological traits change over time.[91] Delayed processing of such data may result in inaccuracies in assessing people's psychological traits.[92] For example, what the TV show *Game of Thrones* indicates about its viewers' personalities in 2011 is quite different from what it does now.[93] Although the television series *Game of Thrones*, when it debuted in 2011, may have indicated that its viewers were more likely to be introverted than extroverted because the show was yet to be popular, the TV show has lost its value as such an indication of psychological traits, given its mainstream status now.[94] Virtual reality helps to overcome this challenge in gathering accurate, actionable insights from delayed processing by doing so in real-time with the most up-to-date meaning.

The second limitation is the depth and sophistication of targeted advertising based on consumer behaviors. Targeted advertising is a form of digital advertising that focuses on specific interests, preferences, and traits of a customer.[95] Advertisers collect this information by tracking customers' activities on the internet and mobile applications.[96] Although social network services such as Facebook and Instagram host targeted advertisements based on the users' recently visited websites or purchase histories, these advertisements do not go beyond targeting a specific brand and items or targeting customers based on broad interest areas or characteristics like age, gender, and products of interest.[97] For example, an online advertising company partnering with a retail clothing website would assign an ID to a customer who visits the retail clothing company's website.[98] Then the online advertising company would assign an ID to that customer, categorizing the customer based on characteristics inferred from the purchase history—age group, gender, and types of clothes purchased.[99]

Virtual reality data would allow companies to produce even more sophisticated and subtle targeted advertisements. For example, virtual reality providers could insert appetizing foods into a virtual reality scene to increase a

[91] *See* Sandra C. Matz, Michal Kosinski, Gideon Nave & David J. Stillwell, *Psychological Targeting as an Effective Approach to Digital Mass Persuasion*, 114 PROC. NAT'L ACAD. SCI. 12714, 12717 (2017).

[92] *Id.*

[93] *Id.*

[94] *Id.*

[95] *What Is Targeted Advertising?*, GCFGLOBAL, https://edu.gcfglobal.org/en/thenow/what-is-targeted-advertising/1/ [https://perma.cc/9APD-XV2T].

[96] *Id.*

[97] *Understanding Online Advertising*, NETWORK ADVISING INITIATIVE, https://www.networkadvertising.org/understanding-online-advertising/how-does-it-work/https://www.networkadvertising.org/understanding-online-advertising/how-does-it-work/ [https://perma.cc/8CWH-KLRT] (describing how individual customers are placed into interest category groups, based on the types of websites visited, their demographics, preferences, and purchase histories).

[98] *Id.*

[99] *See id.*

user's appetite and then feature a targeted advertisement of a restaurant.[100] Moreover, using the physiological detectors in the virtual reality headset, the virtual reality providers could infer each user's real-time mood, spot a vulnerability, and suggest an advertisement that capitalizes on the vulnerability. In other words, advertisements within virtual reality would go a step beyond other social media networks because virtual reality data enables the providers to not only respond to real-time mood of the users but also proactively create certain moods as a subtle form of psychological persuasion.

In sum, virtual reality data has three unique theoretical capacities. First, it can form a self-sufficing data ecosystem, which reduces the need for cumbersome data trading to supplement data for accurate data analysis. Second, given that virtual reality functions as an ideal lab for experiments, virtual reality data is likely to be perceived in the data market as more accurate than other data. However, virtual reality data can nonetheless be distorted because people's behaviors in virtual reality may deviate from reality. Finally, virtual reality data, if processed and applied real-time, allows for more subtle forms of psychological persuasions of virtual reality users.

III. CHALLENGES IN REGULATING VR DATA

Part III examines how the capacity of virtual reality data poses a challenge in regulating it. Part III does so by analyzing Oculus's new Privacy Policy—effective October 11, 2020—and exploring the possible scope and consequences of Oculus's data processing. Then, this Note examines whether Oculus's data processing is GDPR compliant. For interpreting the terms of the GDPR, this Note relies primarily on case law, guidelines from European Data Protection Board ("EDPB"),[101] statements from European Data Protection Supervisor ("EDPS"),[102] and reports from National Data Protection Authorities.

[100] *See* Rogers, *supra* note 66 (noting how eye tracking in virtual reality would help understand a user's reaction to situations in virtual reality, and how this psychological insight allows marketers to in turn shape users' experience in virtual reality).

[101] The European Data Protection Board (EDPB) is an independent European body, which consists of representatives of the national data protection authorities. It adopts general guidance to clarify the terms of European data protection laws, providing a consistent interpretation and application of the laws. It also makes binding decisions towards national supervisory authorities. *About EDPB: Who We Are*, EUROPEAN DATA PROT. BD., https://edpb.europa.eu/about-edpb/about-edpb_en [https://perma.cc/8A2T-UYW3].

[102] The European Data Protection Supervisor (EDPS) is the European Union's (EU) independent data protection authority. Their mission is to "monitor and ensure the protection of personal data and privacy when EU institutions and bodies process the personal information of individuals." *About*, EUROPEAN DATA PROT. SUPERVISOR, https://edps.europa.eu/about-edps_en [https://perma.cc/2G22-C8EN].

A. The Challenge of Aggregate Data

Oculus's new Privacy Policy, under the section "Information You (and Others) Give Us," states that it collects information about "the people, content, and experiences you connect to and how you interact with them across our Oculus Products."[103] Although Oculus does not specify the data collected from such "interact[ions]," it includes both physiological and behavioral information.[104]

Oculus's collection of aggregate data is likely to be considered as biometric data, a special category of personal data that offers more protection for the data subjects.[105] According to the GDPR, personal data refers to (1) any information (2) relating to an identified or identifiable (3) natural person (4) who can be identified *directly or indirectly*.[106] "Directly" refers to being able to identify a person by looking solely at the information that the controller possesses; "indirectly" refers to needing additional information, regardless of whether the controller already holds the additional information or needs another source to identify a person.[107] The GDPR's definition of biometric data clarifies the kind of "indirectly" identifiable data that necessitates heightened protection for the data subjects.[108] According to the GDPR, biometric data is a "personal data *resulting from specific technical processing* relating to the physical, physiological[,] or behavioural characteristics of a natural person, which *allow or confirm* the unique identification of that natural person, such as facial images or dactyloscopic data."[109] The subject of the definition is not just personal data, but also data that has gone through "specific technical processing," such as AI analyses.[110] If such analyses "allow or confirm" identification of a person, then the personal data as a whole would be categorized as "biometric data."[111]

Virtual reality's aggregate behavioral and psychological data is likely to fall under this definition of biometric data. For example, virtual reality data's processing of a collection of body movements, of "how one moves, coordinates and uses one's body segments in relation to each other"[112] may not be "directly" personally identifying but can be "indirectly" identifying as a result of special technical processing, such as AI analyses. The GDPR's definition of biometric

[103] *Oculus Privacy Policy*, *supra* note 22.

[104] *See* Cipresso et al., *supra* note 5, at 3.

[105] *See* GDPR, *supra* note 9, art. 9.

[106] *See id.* at art. 4(1) (emphasis added). For more information on the analysis of the above elements of personal data, see, for example, *What Is Personal Data?*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/key-definitions/what-is-personal-data/ [https://perma.cc/TEL6-LTKQ].

[107] *See What Is Personal Data?*, *supra* note 106.

[108] *See* GDPR, *supra* note 9, art. 4(14).

[109] *Id.* (emphasis added).

[110] *See id.*

[111] *Id.*

[112] Pfeuffer et al., *supra* note 69, at 1. Specifically, the study had a 63.55 percent accuracy rate in identifying the individual by having them point at a target; 49.67 percent for walking. *Id.* at 9.

data is forward-thinking because it includes not just data that is automatically identifying on its own—such as fingerprints or facial recognition—but also behavioral characteristics that are personally identifying in aggregate.

Yet, the question remains as to what level of inference from data would suffice as "allow[ing]" identification of a person and classify that data as biometric data.[113] If, for example, a technical processing of joint movement and coordination has 60 percent accuracy rate of identification, would such data be considered biometric data? EDPB guidelines on biometric data provide a helpful illustration: "[I]t may be possible to infer someone's state of health from the records of their food shopping combined with data on the quality and energy content of foods."[114] Based on this illustration, data generated from virtual reality is likely to be considered as biometric data under the GDPR. The language "may be possible to infer" suggests that the standard of inference for "allow[ing] and confirm[ing]" the identity is not the probability of accuracy of the inference, but the reasonable possibility of such an inference.

Although virtual reality data is likely considered biometric data, such classification may not materially impact the assessment of Oculus's Privacy Policy's compliance under the GDPR. Article 9(1) prohibits the collection of biometric data, but exceptions are enumerated in Article 9(2), one of which is "explicit consent."[115] "Explicit consent" is a GDPR term of art, which sets a higher standard of consent than a regular consent that requires a "statement or . . .clear affirmative action."[116] According to EDPB's May 2020 Guidelines on consent, the exact standard for "explicit consent" is yet to be settled.[117] However, the May 2020 Guidelines do offer helpful examples that qualify as explicit consent.[118] The word "explicit" refers to how the data subject expresses

[113] *Id.* at 2 (evaluating different body motion combinations with regard to their accuracy rate in "allowing" user identification and authentication).

[114] European Data Prot. Bd., *Guidelines 8/2020 on the Targeting of Social Media Users*, ¶ 114 (Sept. 2, 2020), https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_202008_onthetargetingofsocialmediausers_en.pdf [https://perma.cc/2NKG-TBPX].

[115] *See* GDPR, *supra* note 9, art. 9(2)(a).

[116] *Id.* art. 4(11). Granted, even a regular consent is a high bar to meet under the GDPR. A case called *Planet49* clarified the meaning of "freely given" and fully "informed" consent. Planet49, which organized an online promotion lottery, asked the data subject to click on a "participation" button to participate in the lotteries and consent to cookies. The button did not give the opportunity for the data subjects to opt out on the cookies collection. The Advocate General held that clicking on the button did not allow the data subject to make a fully informed consent, because the subjects must have the option to consent for each action. *See generally* Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH, ECLI:EU:C:2019:801 (Oct. 1, 2019).

[117] *See* European Data Prot. Bd., *Guidelines 05/2020 on Consent under Regulation 2016/679*, ¶ 92 (May 4, 2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202005_consent_en.pdf [https://perma.cc/S2PH-DKDG] ("It needs to be clarified what extra efforts a controller should undertake in order to obtain the explicit consent of a data subject in line with the GDPR.").

[118] *See id.* ¶¶ 93–98.

consent[119]: a written statement, a telephone conversation, and an electronic signature qualify as "explicit consent." Even checking a "yes" box as a response to a clear statement on the website, such as "I, hereby, consent to the processing of my data," meets the explicit consent standard.[120] Although certainly more strenuous than the standard for regular consent, explicit consent standard does not seem to pose a huge burden on virtual reality companies, who would only need to create a simple pop-up box with a clear consent statement.[121] Once the users explicitly consent to Oculus's Privacy Notice, they legally allow Oculus to collect personally identifying data.

Of course, simply having an explicit consent from the users does not mean that Oculus can process any data. Article 5(1) lays out the key principles of the GDPR: data minimization and purpose limitation.[122] The data processed must be "adequate, relevant[,] and limited to what is necessary [to achieve the purposes for processing the data] ('data minimization')," and the purpose itself must be "specified, explicit[,] and legitimate . . . ('purpose limitation')."[123] Oculus lists several specified purposes for data collection, such as "[t]o provide and personalize our Oculus Products," and "[t]o improve and develop your experience and our Oculus Products."[124] This language, however, is rather broad. The Policy does not specify exactly which aspect of Oculus Products the company would personalize for its users. In theory, anything—things even beyond a user's imagination—could be personalized based on the language in the Privacy Policy.

Based on a textual interpretation of the GDPR, Oculus's broad language in the Privacy Policy is not likely to pass GDPR's hurdle of "specified purpose." EDPB's Guidelines require a detailed delineation of a "specified purpose":

> The purpose of the collection must be clearly and specifically identified: it must be detailed enough to determine what kind of processing is and is not included within the specified purpose, and to allow that compliance with the law can be assessed and data protection safeguards applied.[125] For these reasons, a purpose that is vague or general, such as for instance "improving users' experience," "marketing purposes," "IT-security purposes" or "future research" will—without more detail—*usually* not meet the criteria of being "specific."[126]

[119] *Id.* ¶ 93.

[120] *Id.* ¶ 96.

[121] *See id.*

[122] GDPR, *supra* note 9, art. 5(1).

[123] *Id.* at (b), (c).

[124] *Oculus Privacy Policy*, *supra* note 22.

[125] Art. 29 Data Prot. Working Party*, Opinion 03/2013 on Purpose Limitation*, at 15 (Apr. 2, 2013), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf [https://perma.cc/KL6Q-M652].

[126] *Id.* at 15–16; *see also* Euopean Data Prot. Bd., *Guidelines 05/2020 on Consent under Regulation 2016/679*, *supra* note 117, at 14 n.30 (emphasis added).

Oculus's language "to improve and develop your experience" and "to provide and personalize our Oculus Products" are exactly the kind of phrases that would *usually* not meet the hurdle of GDPR's "specified purpose" requirement based on EDPB's interpretation.

Yet, the GDPR's policy objective aims for flexibility of rules for new technologies. European Data Protection Supervisor ("EDPS") recently issued a white paper on AI, which states that the GDPR is "technology-neutral" and is "no obstacle for the successful adoption of new technologies, in particular AI."[127] Although the white paper does not directly discuss virtual reality, virtual reality and AI are very closely linked. Virtual reality data needs AI analysis for processing. Moreover, the white paper shows a commitment to flexibility for new technologies in general.[128]

Therefore, it remains to be seen whether Oculus's Privacy Policy would comply with GDPR's "specified purpose" standard. The language in the Policy would *usually* not suffice,[129] but Oculus has a convincing case to be an exception as a leader of the new technology. To ensure full compliance, Oculus could specify the kinds of personalization they offer by listing some concrete examples of personalization in the Privacy Policy while adding the precautionary language that such examples are not exhaustive. However, such a fix still likely would not materially bridge the gap between users' expectations of the consequences of their consent and the actual consequences of their consent.

Bridging this gap poses a legal challenge. Personalizing a user's experience constitutes the very essence of virtual reality service, which is to provide each user an immersive experience akin to the real world.[130] Oculus cannot possibly specify every single dimension of personalization in their Privacy Policy because too many aspects of the service require personalization. Even Oculus may not be able to predict or understand the exact scope of personalization.[131]

[127] European Data Prot. Supervisor, *EDPS Opinion on the European Commission's White Paper on Artificial Intelligence – A European Approach to Excellence and Trust*, ¶ 16 (June 29, 2020), https://edps.europa.eu/sites/edp/files/publication/20-06-19_opinion_ai_white_paper_en.pdf [https://perma.cc/JR7U-846Z].

[128] *See generally id.*

[129] *See Guidelines 05/2020 on Consent under Regulation 2016/679*, *supra* note 117, at 14 n.30 ("[A] purpose that is vague or general, such as for instance 'improving users' experience,' 'marketing purposes,' 'IT-security purposes,' or 'future research' will—without more detail—*usually* not meet the criteria of being 'specific.'") (emphasis added).

[130] *See* Adams, *supra* note 49, at 443.

[131] Controllers of big data like virtual reality data may not be able to predict the exact consequence of their data processing because such controllers use big data precisely to attain patterns and insights not detectable to human eyes. This difficulty of prediction is the reason why the GDPR imposes the duty to carry out "data protection impact assessment," or DPIA. GDPR, *supra* note 9, art. 35(1) ("Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data."). Note that the GDPR only asks for an assessment of what is "likely," and not a precise consequence. *Id.* Moreover, the goal of carrying out DPIA is to create a procedural step for self-assessment tools. *See What is a DPIA?*, INFO.

In a way, virtual reality data exposes the incoherence of the GDPR. Virtual reality service, which by nature requires x-ray-like data from its users to achieve the service goal of immersion, inherently conflicts with GDPR's principles of data minimization and purpose limitation. If the GDPR's "specified purpose" is interpreted strictly—as to necessitate the VR companies to list every possible example of personalization—then no virtual reality company would be able to provide service because it would be impossible to comply with such a requirement, making the companies vulnerable to too many lawsuits. However, if the GDPR, as indicated in their policy objective, remains "flexible" to new technologies like virtual reality, then the GDPR is likely to loosely enforce or lower the standard for "specified purpose," in which case the gap between user expectation and the consequences of user consent would be unbridgeable. Either way, the GDPR is in a bind: this legal quagmire seems difficult to resolve.

B. The Challenge of Highly Accurate but Distorted Data

Another problem with virtual reality data is that it can inaccurately profile people. Although the users' physiological and behavioral tendencies may deviate in virtual reality, such data may nonetheless be used for profiling the users in a hiring process or evaluating their health insurance eligibility. Based on Oculus's Privacy Policy, health companies or recruiters could acquire and use users' data in two ways.

The first way is obtaining the consent of the relevant user. Prominent law firms such as O'Melveny & Myers and consulting companies such as Boston Consulting Group integrated into their hiring process an AI algorithm-based online game platform used to predict candidates' job performance called Pymetrics.[132] Virtual reality is currently also a gaming platform, which means that it is particularly well-suited to evaluate job candidates' task performance.[133]

Virtual reality is likely to be favored over online gaming platforms given its capacity to generate a more in-depth, and perhaps more accurate, evaluation than online games such as Pymetrics.[134] For example, in a job interview taking place in virtual reality, an employer could evaluate the candidate's behavioral characteristics and physical movements—vocal intonation, subconscious body

COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/what-is-a-dpia/ [https://perma.cc/8YSE-6T38]. Although the United Kingdom denies that DPIA is a mere "rubber stamp" and that it is "vital to integrate the outcomes of DPIA" to a project plan, the results from DPIA would not prohibit processing of biometric data. *Id.*

[132] *See, e.g.*, Press Release, O'Melveny & Meyers LLP, O'Melveny Becomes First in Legal Industry to Adopt Next-Generation Technologies that Propel Diversity and Inclusion (Nov. 19, 2018), https://www.omm.com/our-firm/media-center/press-releases/omelveny-adopts-next-generation-technologies-that-propel-diversity-and-inclusion/ [https://perma.cc/WM3M-4F43]; *see also* PYMETRICS, www.pymetrics.ai [https://perma.cc/Z3EE-3P9J].

[133] *See How to Use Virtual Reality and AI in Recruitment: Part 2*, *supra* note 83.

[134] *See id.*

language, thought processing speed.[135] Employers could even test social interaction skills and predict future job performance by designing specific virtual reality challenge scenarios where candidates are asked to interact with virtual customers, products, and environments.[136] Given virtual reality's capacity to provide a ground for multidimensional evaluation of candidates, it would not be surprising if virtual reality companies soon collaborated with programs like Pymetrics for a candidate evaluation service.[137] Yet, such services are likely GDPR compliant, insofar as the companies obtain candidate consent on data collection and processing of their game performance as a part of their job application. Granted, for such service companies to meet the consent requirement in the GDPR, they must ensure that they receive consent not just on participating in the games but also specifically on profiling them.[138]

The second way to profile users is by data trading and obtaining "de-identified" or "aggregate" data from other companies. Oculus's Privacy Policy explicitly states that it will share such data with others.[139] Yet, given that Oculus can collect an x-ray-like data—physical and emotional—about each individual, those "de-identified" or "aggregate" data can still be identifying and used against the users.[140]

Concerningly, the GDPR offers only limited legal protection against profiling. Article 22 of the GDPR, titled "Automated [I]ndividual [D]ecision-[M]aking, [I]ncluding [P]rofiling" states that "[t]he data subject shall have the right not to be subject to a decision based *solely* on automated processing, including profiling, which produces *legal effects* concerning him or her or similarly significantly affects him or her."[141] The plain meaning of the language "solely" suggests that the GDPR only prohibits entirely automated decisions in a hiring process.[142] However, the EDPB Guidelines on Article 22 expands the scope of automated processing: it specifies that automated processing encompasses not just entirely automated decisions but also decisions that lack meaningful human involvement.[143] At the same time, the two examples of prohibited profiling in GDPR Recital 71 restrictively show examples of automatic decisions, such as "automatic refusal of an online credit application or

[135] *See id.*

[136] *See id.*

[137] *See id.*

[138] *See generally* Case C-673/17, Bundesverband der Verbraucherzentralen und Verbraucherverbände – Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH, ECLI:EU:C:2019:801 (Oct. 1, 2019).

[139] *Oculus Privacy Policy*, *supra* note 22.

[140] *See* Lenz, *supra* note 6, at 21–22.

[141] GDPR, *supra* note 9, art. 22(1) (emphasis added).

[142] *See id.*

[143] Art. 29 Data Prot. Working Party, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679*, at 8 (Feb. 6, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053 [https://perma.cc/Z3V5-YXQB].

e-recruiting practice without any human intervention."[144] Given the lack of clarity on what constitutes a meaningful human involvement, virtual reality users are vulnerable to profiling.

Moreover, the kind of prohibited profiling that has "legal effects" concerning data subjects includes "discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect."[145] The language seems to offer protection to groups who are historically vulnerable to discrimination but not to the subtle propensities reflected in virtual reality game performance. This lack of protection opens the door for AI and virtual reality-based hiring practices to develop and continue.

Although data from virtual reality may be relatively more accurate than other gaming platforms, profiling based on virtual reality data is still concerning, given that the data captures how the user behaves in a virtual world, not the real world.[146] Yet, the GDPR does not provide clear guidance on the level of accuracy required to profile data subjects. It merely states that data controllers "should use *appropriate* mathematical or statistical procedures for the profiling . . . to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised."[147] The phrase "appropriate . . . procedures" indicates that inaccuracies from data could be GDPR compliant, as long as it is procedurally satisfactory.[148] As noted above, the strength of virtual reality data lies in its procedural perfection, given its ability to repeat identical simulations. In sum, the current languages in the GDPR do not seem to adequately protect data subjects whose behaviors in virtual reality would deviate from actual reality. Yet, they are profiled nonetheless based on their performance within the virtual world.

C. The Challenge of Subtle Psychological Manipulation

Another challenge of virtual reality data is its capacity to help produce subtle psychological persuasions.[149] Although Oculus's Privacy Policy does not explicitly state that it would market or help others market commercial products not directly related to Oculus, such activities could be GDPR compliant. Oculus's Privacy Policy indicates that Oculus will take advantage of the technology to do so.[150] It explicitly states that it collects data to "market to" its

[144] GDPR, *supra* note 9, recital 71.

[145] *Id.*

[146] Again, even if the data is perfectly accurate, the fact that virtual reality data can reveal such intimate details of an individual's life in and of itself poses privacy concerns. For more discussion, see *infra* Part III.D.

[147] GDPR, *supra* note 9, recital 71.

[148] *See id.*

[149] *See supra* Part II.C.

[150] *See Oculus Privacy Policy*, *supra* note 22.

users, to "send . . . promotional messages and content about Oculus Products and Oculus-related experiences on and off our Oculus Products," and to "use this information to measure how users respond to our marketing efforts."[151] Oculus's data would be available not only to Oculus but also to other companies that provide marketing services for Oculus.[152]

The GDPR allows for data collected to be processed for purposes "compatible" with initial purposes.[153] Although the GDPR does not define what qualifies as "compatible," member states have each interpreted the meaning of compatibility. For example, UK's Information Commissioner's Office states that whether a purpose is compatible is an issue of fairness, or the data subject's "reasonable expectation" that their data could be used in this way.[154] On the surface, the reasonable expectation standard seems to be a possible solution to the criticisms against consent-based regulations like the GDPR—that the consent is a mere rubber stamp because the controllers could use the data beyond ordinary users' expectation. If virtual reality is strictly viewed as a gaming platform, harvesting users' data to market other commercial products while playing VR games may be beyond a user's reasonable expectations.[155]

However, virtual reality is effectively becoming another platform for social network services (SNS).[156] Virtual reality is a space not only to play games but also to build another community and express oneself. The more data subjects view virtual reality as another form of social network service, the more the processing of marketing data falls within reasonable expectations because SNS is already providing tailored advertisements. Then, extending the scope of marketing activities seems to be compatible with the original purpose.

The meaning of reasonable expectation of the data subject—as a standard for determining a "compatible purpose"—also depends on how an Advocate General of the member states or EDPB in the future would conceptualize virtual reality.[157] On the one hand, if an Advocate General viewed virtual reality as a conceptual equivalent of a real world, then users should reasonably expect that

[151] *Id.*

[152] *See id.*

[153] GDPR, *supra* note 9, recital 50 ("The processing of personal data for purposes other than those for which the personal data were initially collected should be allowed only where the processing is compatible with the purposes for which the personal data were initially collected. In such a case, no legal basis separate from that which allowed the collection of the personal data is required.").

[154] *What is the "Legitimate Interests" Basis?*, INFO. COMM'R'S OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/what-is-the-legitimate-interests-basis/#reasonable_expectations [https://perma.cc/4KJ2-UGXC].

[155] Even games, which are increasingly social and converging with social networks, are becoming a key source of data harvesting for marketers. *See* O'Brolcháin, *supra* note 5, at 3 ("The Idea of 'Gamification', i.e., making day-to-day activities resemble games by awarding points or similar and recording these on apps and SNs, further illustrates the impact of Internet technologies on everyday life: the providers of the 'games' profit by gathering data on the players.").

[156] *See generally id.*

[157] Currently, there is no case law precedent or EDPB guideline on virtual reality.

their data would be harvested to feature real world-like advertisements. On the other hand, if an Advocate General were to interpret virtual reality as a fundamentally different creation from the real world, then users would have a drastically different expectation of the kind of data collected in virtual reality.

Moreover, if an Advocate General were to apply the uniform standard of "reasonable expectation" for all users, then another problem would arise because such a standard can lead to inequitable results. Users have widely different expectations and ideas about what virtual reality data can do: diehard techies may be fully informed on the possible ramifications of virtual reality data processing, whereas those one-time users who experienced the service using a friend's VR headset may not be so informed. Given the information gap among the data subjects, reasonable expectation of the data subject is not a panacea to the problem of consent-based regulatory models like the GDPR.

D. VR Data: The Overall Challenge against the GDPR

Overall, virtual reality data possesses a unique capacity as a self-sufficing data ecosystem that enables in-depth predictive analysis and timely application. In the wake of this capacity, the languages in virtual reality companies' Privacy Policy would obtain new meanings unfathomable to many of its users. Privacy risks of sharing "de-identified" or "aggregate" data are one such example. A more telling example is the section on the purpose of data collection.[158] Oculus's policy states:

> "We use the information we collect to provide you with our Oculus Products, [to] [c]ustomize your experiences on our Oculus Products based on your activities, including the content, games, apps, and other experiences you interact with, the other online services you use, and other information we collect. This allows us to make your experience unique and relevant to you, for example by showing you content that is most relevant to you."[159]

The phrase "unique and relevant to you" seems like an ordinary language that is necessary to provide a seamless service. Users reading the phrase are likely to assume that the experience "unique and relevant" to them would be based on the users' own perception of who they are, or if not, at least an experience cognizable to them as relevant.

However, the immersive nature of virtual reality allows companies to offer subtle and sophisticated personalization unrecognizable to users. One example is ambient conditions or atmospherics.[160] Atmospherics is "the effort to design buying environments to produce specific emotional effects in the buyer that

[158] *See Oculus Privacy Policy*, *supra* note 22.

[159] *Id.*

[160] Pierański & Strykowski, *supra* note 19, at 190 (describing how ambient elements influence consumers on a more subconscious level and how virtual reality allows companies to design atmospheric elements, such as visual and aural, with ease).

enhance purchase probability."[161] The atmospheric dimensions include visual, aural, olfactory, tactile, and taste.[162] Currently, virtual reality technology easily enables visual and aural personalization and is making promising progress toward tactile.[163] Visual, aural, and tactile personalization in virtual reality is powerful because in order for atmospherics to have influence on a consumer, the atmospheric has to strike the right balance of neither being too intense nor too low.[164] At the same time, atmospherics only exist in the background stimuli of the virtual world and it is difficult for users to detect that the atmospherics—such as color of the floor, volume of the music—is personalized based on their tolerance level.[165]

In fact, the personalization must go unnoticed for the virtual world to appear as realistic as possible, which is the purpose of virtual reality. For example, if users were to become aware of the details of the personalization, such as ambience tuned to their needs, such awareness would distract users from being completely immersed to the virtual world. Therefore, not only are companies incentivized to offer unrecognizable personalization but also users are incentivized to be blind to personalization to fully enjoy the benefits of virtual reality.

In short, virtual reality is unique in that it not only has the capacity to provide unrecognizable personalization, but it must also do so, by its conceptual definition, to achieve its purpose. The corollary is that the extent of personalization and their possible impacts on privacy remain hidden to users who consented to the service. This gap between the users' understanding of their consent and the actual implication of consent undermines the right to self-determination, which is embedded in the GDPR.[166] The right to self-determination protects our autonomous capacity to shape, define, and express who we are.[167] Although human beings, as social animals, shape and are shaped by one another, the notion of self-determination respects individuals to ultimately choose what to incorporate into their identities. Right to self-

[161] *Id.*

[162] *See id.*

[163] *Id.* at 190–91 ("VR allows one to choose from an almost unlimited range of colors and lighting levels; as well as something that especially creates new possibilities, the size and shape of store fixtures. Another dimension is the aural. The appropriate music can be played not through speakers as it is in bricks-and-mortar stores but through earphones. The latest technology developments seem to be very promising in the area of including the tactile dimension in VR. More and more sophisticated virtual gloves are available on the market that make it possible for instance to feel the texture or weight of a given product.").

[164] *Id.* at 191.

[165] *Id.* at 190, 192.

[166] *See* Paul M. Schwartz & Karl-Nikolaus Peifer, *Transatlantic Data Privacy Law*, 106 GEO. L.J. 115, 123 (2017) ("In the EU, data protection is a fundamental right anchored in interests of dignity, personality, and self-determination.").

[167] *See id.* at 140 ("Self-determination protects autonomy. But the selling and transferring of personality rights by a data subject can alienate these interests in a fashion that makes her an object for the data processor.").

determination presupposes that the data subjects dictate what is meaningful to them. Therefore, the ability of virtual reality providers to shape the users' identity without the users' recognition fundamentally challenges the right to self-determination and autonomy. Yet, these key rights remain an important value to people today, especially in the context of privacy. Although privacy has many meanings, common themes shape our collective view of the purpose of privacy, such as the need to preserve personal dignity and develop personal autonomy.[168]

IV.
Solution

Ultimately, the age of virtual reality necessitates reimagining the means to uphold the key rights that the GDPR strives to protect, such as the right to self-determination, autonomy, and sovereignty.[169] But text-based informed consent is an outdated mode of protecting these rights. Rather, virtual reality data collection permeates insidiously and subtly—sometimes in ways beyond human recognition and sometimes in ways within human recognition but posed as an innocuous or a negligible event. The text, such as privacy policies, is an inadequate medium to effectively communicate these subtle dangers to virtual reality users.

One lesson to draw upon in reimagining the means to uphold the data subjects' rights is the Kodak moment. The Kodak moment illustrates a possible solution to when a revolutionary technology drastically reshapes what is private, yet people's expectations of privacy lag behind.[170] A portable Kodak camera, which allowed taking photos in public, spurred great fear and anxiety when it was first introduced because cameras until then were for moments in the private realm. It was clear that the population's expectations of privacy had yet to catch up with the revolutionary technology.[171] In response, the government introduced a drastic measure of temporarily banning the use of Kodak camera in public places, such as resort beaches and the Washington Monument, to allow for social norms to catch up to the new technology.[172] Of course, the privacy challenges that the virtual reality poses are distinct from those posed by Kodak. The privacy consequences of the photos from Kodak are more intuitive to ordinary users than those of virtual reality data as the collection process remains invisible to the users. Despite this difference, however, the Kodak moment shows that some creative solutions beyond just textual revisions of policies must take place to bridge the gap between the user expectation and the actual privacy risks.

[168] *See* Shapiro et al., *supra* note 18, at 24.

[169] *See* Schwartz & Peifer, *supra* note 166, at 123.

[170] *See* Elaine Sedenberg, Richmond Wong & John Chuang, A Window into the Soul: Biosensing in Public 6 (May 10, 2018) (unpublished manuscript), https://arxiv.org/pdf/1702.04235.pdf [https://perma.cc/V3C7-KHND].

[171] *Id.* at 6–7.

[172] *Id.* at 7.

This Section proposes two possible, but not exhaustive, solutions to uphold the users' right to self-determination in the context of using virtual reality. The first solution is to require virtual reality companies to allow the users to control their privacy settings so that users can choose their level of customized experience based on the users' unique characteristics. Virtual reality technology is constantly evolving to provide a more personal experience to its users. For example, some have already experimented with influencing a user's mood by measuring the user's heartbeat through a sensor and changing the background light in virtual reality to "a more soothing blue" when the heart rate increases.[173] The customization that responds to one's emotional state is helpful in the context of treatment for anxiety and other mental health issues.[174]

At the same time, however, such a customization can endanger a user's sense of autonomy and the ability to shape their own identity. Regulating personal boundaries is a key mechanism to shaping one's identity and developing autonomy.[175] However, virtual reality can subtly invade this personal boundary by providing more information about the users than the users may wish to know.[176] Not everyone is always aware of their emotional and cognitive states, and sometimes they may not even want to be aware for various personal reasons. Having virtual reality customized to reflect individuals' emotional states means that the users are forced to recognize and confront their own fears. For instance, a color change to a "soothing blue"[177] in the virtual background reflects a direct manifestation of their heart rate, which is physiological evidence of one's anxiety or fear. This customized experience based on the users' bio-signals, such as a heart rate, can have an immense aggregate effect in shaping one's identity. Unlike external subjective opinions about the users, which the users could ignore or control more easily, the users are more likely to perceive bio-signals such as heart rates to be an objective, valid evidence of their tendencies, lending credibility to what virtual reality subtly indicates about them. For example, if a user's heart beats faster than others in a similar game quest in virtual reality, and if their customized virtual reality reflects this reality, then the user may begin to consider themselves unconsciously or consciously as too reactive or vulnerable.

Providing customizable privacy settings—such as how much physiological data each user wants to permit to create their immersive experience—would allow control over the extent to which the users wish their identities to be shaped

[173] Javier Soto Morras, *Creating a Customized VR Experience*, IDEO (Oct. 2, 2016), https://www.ideo.com/blog/creating-a-customized-vr-experience [https://perma.cc/6SRZ-HPZ2].

[174] *See id.*

[175] *See* Kelly Quinn, *An Ecological Approach to Privacy: Doing Online Privacy at Midlife*, 58 J. BROAD. & ELEC. MEDIA 562, 564 (2014).

[176] This is a more invasive form of personalization than adjusting ambience settings that is designed to go unnoticed by users. Whether to introduce a more invasive personalization, which may come at the sacrifice of less immersive user experience and undermine the goal of virtual reality, is likely a commercial calculation.

[177] Morras, *supra* note 173.

by virtual reality. Social network services such as Facebook already allow their users to manage their privacy settings.[178] Options of control include limiting profile access, blocking and hiding site users, and item-level access control.[179] Through the exercises of maintaining and negotiating boundaries with others on Facebook, Facebook users dictate whom to influence and by whom to be influenced.[180] Similarly, virtual reality users would gain a sense of control by managing their privacy settings. For example, a privacy setting could include the intensity of interactions in virtual reality and the extent of incorporating user bio-signals to customize the virtual reality world.

Yet, this solution is more difficult to implement in virtual reality than in social media for several reasons. First, privacy settings in social media are geared toward boundary control of interpersonal relations, limiting the scope of audience to one's profile.[181] The downside of limiting access to one's profile is fewer meaningful interactions with other people. However, this limited access would not significantly compromise the purpose of social media as a networking platform. Contrastingly, controlling the privacy settings in virtual reality could compromise the main function of virtual reality, which is to provide a real-world like immersive experience. The more a user limits the level of customization based on the user's unique characteristics, the less virtual reality would appear real to the user. In a way, restricting customization would defeat the purpose of experiencing virtual reality.

Another potential problem is the disparity between reported privacy attitudes and observed privacy behaviors called the "privacy paradox."[182] One of the causes of the privacy paradox is the lack of awareness and understanding of privacy risks: one would assess a certain privacy risk as negligible, when in fact it could have far-reaching questions.[183] For example, few users would evaluate that a virtual reality background automatically changing to a calming blue to reflect one's emotional state would pose a significant privacy risk. Some would even consider it "cool." The caveat is that these individual features, in aggregate, could have long-reaching consequences that undermine autonomy.

Therefore, a meaningful solution to uphold privacy rights would also address the causes of privacy paradox. One solution that would complement customizable privacy settings would be to require users, prior to their consent,

[178] *See generally* Fred Stutzman & Jacob Kramer-Duffield, *Friends Only: Examining a Privacy-Enhancing Behavior in Facebook*, *in* 3 CHI '10: PROCEEDINGS OF THE SIGCHI CONFERENCE ON HUMAN FACTORS IN COMPUTING SYSTEMS 1553 (2010) (examining boundary regulation on content-sharing social network platforms like Facebook).

[179] *Id.* at 1553.

[180] *See id.*

[181] *See id.*

[182] *Id.*

[183] *See generally* Susanne Barth & Menno D.T. de Jong, *The Privacy Paradox – Investigating Discrepancies Between Expressed Privacy Concerns and Actual Online Behavior – A Systematic Literature Review*, 34 TELEMATICS & INFORMATICS 1038 (2017).

to watch a short video and engage in interactive exercises that educate the users of the possible consequences of virtual reality data. Doing interactive exercises, which tests users' comprehension of the video presented, would prevent users from scrolling down without reading the privacy policy. Other fields that collect and process personal data, such as the field of medicine, are now devising a more interactive platform to bridge the gap between the patients' expectation of consequences from the procedures and the actual consequences.

For example, Yale School of Medicine developed Virtual Multimedia Interactive Informed Consent (VIC), which is a digital health tool that utilizes virtual coaching by featuring a multimedia library that teaches the risks and benefits of a clinical study.[184] They devised this platform because 44 percent of participants who sign informed consent documents in a clinical trial setting do not understand the nature of the proposed procedure.[185] It conceptualizes informed consent as an interactive learning process, rather than a one-time reading of a text-based privacy policy.[186] The interactive process includes videos, illustrations, and answering quiz questions for review.[187] The patients in the study found the interactive tool easy to use and succeeded in doing tasks assigned by the tool.[188]

Applying these interactive tools prior to using virtual reality would help address some limitations of text-based informed consent. A picture is worth a thousand words; watching a video once could stimulate users' imagination in ways that reading a dense and long text cannot. The privacy paradox exists because the users are often unaware of the magnitude of the privacy risks. Yet, users are not motivated to read through privacy policies because they live in a busy world and privacy risks seem negligible to them. Therefore, data privacy regulations should focus on introducing solutions that realistically factor in the motivations of the users. Interactive platforms, combined with controlling privacy settings, would motivate the users to sit down and think through the ramifications of their virtual reality experience, in ways that a text-based privacy policy cannot.

[184] Yale Sch. of Med., *Virtual Multimedia Interactive Informed Consent (VIC)*, ABUJARAD'S DIGIT. HEALTH LAB (Oct. 2, 2021), https://medicine.yale.edu/lab/abujarad/projects/VIC/ [https://perma.cc/3BLU-2FYN].

[185] *Id.*

[186] *Id.*

[187] *See* Fuad Abujarad, Sandra Alfano, Tiffani J. Bright, Sneha Kannoth, Nicole Grant, Matthew Gueble, Peter Peduzzi & Geoffrey Chupp, *Building an Informed Consent Tool Starting with the Patient: The Patient Centered Virtual Multimedia Interactive Informed Consent (VIC)*, 2017 AMIA ANN. SYMP. PROC. 374, 375.

[188] *Id.* at 376.

CONCLUSION

Ralph Waldon Emerson once powerfully said, “All life is an experiment. The more experiments you make, the better.”[189] This analogy of life urges the audience to undertake new challenges without the fear of consequences. Virtual reality allows users to do precisely this by providing them a safe space to explore, interact, and engage with a different world without facing the real-life dangers that typically accompany such experiments.

But the experiments also come with privacy risks, risks that are not obvious to users. What distinguishes virtual reality from other IoTs is its ability to provide an immersive experience in a different world. To provide as realistic experience as possible, virtual reality companies must personalize the service, using data such as eye movements to sync the virtual world to the user’s view. And the more data virtual reality companies collect and process from users, the more personalized and “real” the virtual world—the sensation, the interaction, and the story—feels to users. By definition, virtual reality necessitates collecting and processing extensive data to achieve its purpose. And by definition, the personalized aspects of virtual reality enabled by that data must be as unnoticeable as possible to not distract the users from the immersive experience. Because this sophisticated personalization goes unrecognized by users, the accompanying privacy risks also go unnoticed.

This Note has argued that texts such as privacy policies—even if fully read by users, which is seldom done—fail to fully communicate the nature of virtual reality’s privacy risks. The unique capacities of virtual reality allow companies to identify, respond to, and shape users’ unconscious needs and behaviors. This knowledge shift—that the companies may know the user better than the user knows themselves—transforms ordinary privacy policy languages on the personalized service like providing “experience relevant and unique to you.” What companies find relevant to users may be beyond the grasp of what users find to be relevant to themselves. Given the inadequacy of text-based informed consent, this Note has instead suggested other solutions, such as visualizing privacy risks through interactive videos and customizable privacy settings, for users to more consciously weigh the benefits and risks of using virtual reality.

All life is an experiment. The more experiments you make—understanding the risks and facing them head on—the better.

[189] Ralph Waldo Emerson, Entry on Nov. 11, 1842, *in* THE HEART OF EMERSON’S JOURNALS 198 (Bliss Perry ed., 1995).