2023

Political Advertising in Virtual Reality

Scott P. Bloomberg

POLITICAL ADVERTISING IN VIRTUAL REALITY

Scott Bloomberg[*]

TABLE OF CONTENTS

I. INTRODUCTION

A range of reactions met Mark Zuckerberg's 2021 announcement that The Facebook Company would rebrand as "Meta" and would adopt, as its primary strategic focus, the creation of a virtual reality ("VR") environment[1] called the

[*] Associate Professor of Law, University of Maine School of Law. I thank the attendees of the 2022 Privacy Law Scholars Conference—where an earlier version of this Article was presented—and the participants in Maine Law's Faculty Workshop Series, for their feedback on the Article. I also thank the Stanford Cyber Policy Center for inviting me to present this paper at the Existing Law and Extended Reality Symposium. Thank you to Ethan Zuckerman, Brittan Heller, and Avi Bar-Zeev for taking the time to discuss earlier drafts of this article, and to Alexandra Roberts, Thomas Kadri, Hany Farid, and Tamar Katz for sharing sources that deepened my understanding of the issues addressed in the Article. Last but not least, I thank Dale Rappaneau and Mark Sayre for their superb research assistance, and the *FALR* staff for their editorial work.

[1] Virtual reality ("VR") is "a fully immersive software-generated artificial digital environment [that is] . . . experienced by users via special electronic equipment, such

Metaverse.[2] Some commenters questioned the company's motive for announcing the rebranding, noting that Facebook badly needed a change in narrative after the Facebook Papers leaks and other scandals.[3] Others noted that the idea of creating a metaverse-like environment was nothing new and had in fact been done before.[4] Some thought Meta's Metaverse was a terrible, dystopian idea.[5] Others were enthusiastic about the economic aspects of Mark Zuckerberg's vision.[6]

Good idea, bad idea, old idea, or new idea; one thing is certain: When one of the world's wealthiest technology companies announces a plan to focus its considerable resources on developing a new-verse, it is time to focus a critical lens on that plan. For privacy law scholars, there is much on which to focus. Operating a VR environment like the so-called metaverse will involve the collection, processing, storage, and sharing of vast quantities of personal data.[7] That data will likely range from

as a Head Mounted Display (HMD)." *Virtual Reality (VR)*, XR SAFETY INITIATIVE, https://xrsi.org/definition/virtual-reality-vr (last visited Mar. 2, 2023). The term "immersive reality" is sometimes used interchangeably with VR.

[2] Facebook Reality Labs, *Mark Zuckerberg Keynote Address at Facebook Connects 2021* (Oct. 28, 2021), https://www.facebook.com/facebookrealitylabs/videos/561535698440683/.

[3] Peter Suciu, *A 'Metaverse' Of Questions: What's Behind Facebook's Rebranding?*, FORBES (Oct. 23, 2021), https://www.forbes.com/sites/petersuciu/2021/10/23/a-metaverse-of-questions-whats-behind-facebooks-rebranding/?sh=29a1091c3be1; *e.g.*, James D. Walsh, *Why Facebook's Metaverse Is Dead on Arrival*, N.Y. MAG. (Nov. 8, 2021), https://nymag.com/intelligencer/2021/11/why-facebooks-metaverse-is-dead-on-arrival.html.

[4] Ethan Zuckerman, *Hey, Facebook, I Made a Metaverse 27 Years Ago*, THE ATLANTIC (Oct. 29, 2021), https://www.theatlantic.com/technology/archive/2021/10/facebook-metaverse-was-always-terrible/620546/; Jeff Grubb, *Facebook Stops Just Short of Rebranding to 'The Web'*, VENTUREBEAT (Oct. 28, 2021), https://venturebeat.com/arvr/facebook-stops-just-short-of-rebranding-to-the-web/; Louis B. Rosenberg, *Regulating the Metaverse, a Blueprint for the Future* (2022), https://www.researchgate.net/publication/362541437_Regulating_the_Metaverse_a_Blueprint_for_the_Future (Indeed, the term "metaverse" is not unique to Meta-née-Facebook, or to any specific company. It is a generic term used to describe "a persistent and immersive simulated world that is experienced in the first person by large groups of simultaneous users who share a strong sense of mutual presence.").

[5] Brian Merchant, *The Metaverse Has Always Been a Dystopian Idea*, VICE (July 30, 2021, 9:00AM), https://www.vice.com/en/article/v7eqbb/the-metaverse-has-always-been-a-dystopia.

[6] Michel Kilzi, *The New Virtual Economy of the Metaverse*, FORBES (May 20, 2022), https://www.forbes.com/sites/forbesbusinesscouncil/2022/05/20/the-new-virtual-economy-of-the-metaverse/?sh=72cdb91246d8.

[7] David Uberti, *Come the Metaverse, Can Privacy Exist?*, WALL ST. J. (Jan. 4, 2022), https://www.wsj.com/articles/come-the-metaverse-can-privacy-exist-11641292206 ("The infrastructure underpinning the metaverse—virtual-reality glasses and augmented-reality software, for openers—will rely on reams of data showing how users interact with their surroundings . . . .").

basic account information to highly sensitive information that tracks how users interact with their virtual surroundings.[8] And beyond information-privacy issues, VR raises important privacy-related questions involving equality and bodily autonomy. For instance: Will people be able to grope your body (or, more specifically, the avatar that represents your body) in VR?[9] What real-world inequities will carry over into our new virtual spaces?[10]

Privacy scholars (and others) are just beginning to grapple with one particularly vexing problem that promises to be endemic in VR environments: advertising. Renowned computer scientist Louis Rosenberg has called VR platforms "the most dangerous tool of persuasion that humanity will have ever created."[11] And with good reason:

> [VR] platforms will be able to track where you go, what you do, where you look and how long your gaze lingers, your gait; they'll look at your posture and be able to infer your level of interest. They'll monitor your facial expressions, vocal inflections, vital signs, blood pressure, heart rate, blood flow patterns on your face. These extensive profiles will make the amount of information that the social media companies get seem like the good old days.[12]

VR platforms will be able to use this biometric data—acquired through biometric monitoring devices incorporated into VR technologies—to target advertisements to users in unprecedented ways. In her 2020 article, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, Brittan Heller labels this advertising

[8] *Id.*; *see also infra* Part III(A).

[9] *See* Mary Anne Franks, *The Desert of the Unreal: Inequality in Virtual and Augmented Reality*, 51 U.C. DAVIS L. REV. 499, 501–02 (2017) (citing Jordan Belamire, *My First Virtual Reality Groping*, MEDIUM (Oct. 20, 2016), https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee (recounting the experience of a female gamer whose avatar was groped by another player during a game).

[10] *See id.* at 503 (warning against the carry-over of existing inequalities into virtual reality).

[11] Derek Robertson, *'The Most Dangerous Tool of Persuasion,'* POLITICO (Sept. 14, 2022, 4:00 PM) (quoting Louis Rosenberg), https://www.politico.com/newsletters/digital-future-daily/2022/09/14/metaverse-most-dangerous-tool-persuasion-00056681.

[12] *Id.* (quoting Louis Rosenberg).

practice "biometric psychography."[13] She explains that VR technologies rely (and will increasingly rely) on monitoring users' bodies in order to function.

> [A]n immersive system must understand how users interact with the world at a foundational level. For example, any immersive system must track what its user looks at and for how long. It can implicitly track how individuals react to things - do they stare? Do they do a double take? Do they resolutely look away?[14]

Heller, like Rosenberg, posits that companies will be able to gain valuable insights from tracking the ways users' bodies react in VR environments. Companies could then use these insights to target advertisements to users or for other commercial ends. This "gathering and use of biological data, paired with the stimuli that caused a biological reaction, to determine users' preferences, likes, and dislikes," is biometric psychography.[15]

If this sounds like science fiction, it is not. VR platforms have a tremendous financial incentive to adopt advertising-centric business models that rely on accurately predicting users' preferences. VR technologies already incorporate biometric monitoring devices. And companies are already using biometric data to conduct consumer research through controlled studies and to serve display advertisements in the brick-and-mortar context. Just as internet platforms turned the troves of data they acquired by surveilling users' online behaviors into valuable advertising products, VR platforms may soon use data about how you interact in VR environments to serve you ads. Extant problems with online ad microtargeting thus threaten to carry over, and worsen, as VR technologies gain more widespread adoption.

While scholars have indeed begun focusing on the dangers of *commercial* advertising in VR, they have largely overlooked how these same technologies will enable the extreme microtargeting of *political* advertisements using biometric and other highly personal data. And it would border on naiveté to think that political campaigns will not try to use the "most

[13] Brittan Heller, *Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law*, 23 VAND. J. ENT. & TECH. L. 1, 4 (2020).
[14] *Id.* at 10.
[15] *Id.* at 6.

dangerous tool of persuasion" to persuade—and manipulate—how people vote: Political campaigns readily adopted, and now rely upon, the microtargeting tools provided by existing internet platforms, and innovative campaigns are already experimenting with VR and related technologies. In the not-so-distant future, we may be seeing and hearing political advertisements based in part on what our involuntary biological reactions reveal about our preferences and dislikes. As a consequence, each of us will experience the messaging differently. On granular levels, people may see candidates wearing different clothing (a suit or a plaid shirt?) or driving in different automobiles (a minivan or a pickup truck?). On higher levels, people attending the same political rally may be privy to different speakers, or different topics of speech, or even different speeches from the same speaker. The political ads we see might also be displayed, tested, and adjusted based on what our faces, eyes, bodies, and other personal data reveal about our preferences.

To some degree, this type of fractured informational environment already exists on the internet.[16] Through the advertising tools that platforms originally designed for commercial use, candidates can slice-and-dice their audiences, tailoring different messages to different segments of the population based on various types of personal information.[17] That practice has led to a number of challenges for our democracy, including abuses by nefarious actors, the creation of filter bubbles, challenges to presenting counter-speech, the erosion of shared truths and norms, and invasions on intellectual and political privacy.[18] If targeting ads in VR using biometric psychography becomes the next step in the evolution of political advertising, these problems will only get worse.

Nonetheless, a formidable obstacle awaits policymakers who try to curb this ad-targeting practice: The Supreme Court's First Amendment jurisprudence. Litigants will be able to use the Supreme Court's current, libertarian, Speech Clause doctrine to cast restrictions on the use of biometric psychography (and other microtargeting techniques) in VR political advertising as severely burdening core political speech rights, just as they have done with respect to campaign finance restrictions. A reviewing court would subject such restrictions to strict scrutiny and would almost certainly find that they violate the First Amendment.

[16] *See infra* Part II(B) (discussing political ad microtargeting).

[17] *Id.*

[18] *Id.*

And, as I shall explain, even content-neutral laws that restrict the general use of biometric psychography would be vulnerable to as-applied challenges under current Speech Clause doctrine.

Part II of this Article explains how online platforms' business models revolve around the use of personal information to target advertisements based on users' predicted preferences. This Part also describes how political campaigns have leveraged these advertising products and details the democratic problems that stem from microtargeting political advertisements. Part III theorizes how political advertising will work in VR environments. This Part unpacks the prospect of biometric ad targeting in VR; identifies three forms of political advertising that may arise in VR environments; and—by describing a hypothetical VR political rally—illustrates how using biometric data to target VR political ads will greatly exacerbate current problems caused by online political ad microtargeting. Part IV analyzes how laws restricting the use of biometric data to target VR political advertisements would fair under the Supreme Court's current, libertarian, First Amendment jurisprudence. That analysis reveals that content-based restrictions are almost certain to violate the Speech Clause and that even content-neutral restrictions would be susceptible to as-applied challenges from political advertisers. Part V concludes the Article by discussing the consequences of its First Amendment analysis.

II. Political Advertising on Online Platforms

A. Problems with the Platform Ad Targeting Business Model

There is a social media platform for everyone these days. If you're into short, humorous videos—TikTok; glamorous photos of people living the good life—Instagram; quips from people you find interesting—Twitter; communities built around common interests—Reddit; staying in touch with family and friends—Facebook; a more professional vibe—LinkedIn. Snapchat. YouTube. Pinterest. The list goes on.

For all the different permutations of social media platforms out there, the platforms' business models largely revolve around the same thing: advertising.[19] Advertising

[19] During a hearing before the Senate's Commerce and Judiciary committees, Mark Zuckerberg famously (or infamously) declared, "Senator, we run ads," in response to Senator Chuck Grassley's question of how Facebook is able to "sustain a business model in which users don't pay for your service." *Transcript of Mark Zuckerberg's Senate Hearing*, WASH. POST (Apr. 10, 2018), https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/. *See also* Kate Klonick, *The New Governors: The*

generates tremendous revenue for platforms. It is what drives their now-astronomical market values.[20]

The value proposition that platforms offer to marketers derives from the information that platforms are able to harvest from their users. Some of that information is run-of-the-mill personal information that users submit when they initially create a profile to join the platform: name, age, gender, place of residence, job, and the like. But much of the information comes from how users engage with the platforms. When a user posts content, associates with people or groups, or interacts with the platform through likes, dislikes, upvotes, downvotes, retweets, shares, comments, etc., that engagement can be tracked, databased, and analyzed to produce insights about which advertisements the user should be shown.[21] And which advertisements should the user be shown? The advertisements they are most likely to click, and thus generate revenue for the platforms, of course.

Platforms' advertising systems run on predictions. The more accurately a platform can predict which advertisements a user will click, the more money the platform will make. And the more information a platform has about its users, the more accurately it can predict their users' behavior.[22] To illustrate how this works, assume that a platform knows nothing about a user and simply displays random advertisements to the user. The user may—by happenstance—click an ad that interests them, thus causing the advertiser to pay the platform a small price for the click. But it may take 10,000 ads before the user actually clicks on one; the click-through-rate ("CTR") may be 0.01%. Now assume that the platform knows the user's profile information. It knows the user is a 30-year-old female law student in Portland,

People, Rules, and Processes Governing Online Speech, 131 HARV. L. REV. 1598, 1627 (2018) (describing how the desire to maximize advertising revenues drives social media companies' content moderation decisions).

[20] *See, e.g.,* Sam Shead, *Facebook is the Big Loser of the Fourth Quarter's Advertising Wars,* CNBC (Feb. 4, 2022, 8:55 AM), https://www.cnbc.com/2022/02/04/facebook-is-the-big-loser-of-the-fourth-quarters-advertising-wars.html (highlighting the relation between social media companies' advertising revenues and their market valuations).

[21] There is a robust body of literature regarding how social media companies collect personal information to engage in behavioral and other advertising practices. For a few examples that are particularly relevant to this article, *see* SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM (2019); TIM WU, THE ATTENTION MERCHANTS 323–27 (2016); Dawn Carla Nunziato, *The Varieties of Counterspeech and Censorship on Social Media*, 54 U.C. DAVIS L. REV. 2491, 2537–52 (2021).

[22] *See, e.g.*, Kyle Langvardt, *Regulating Habit-Forming Technology*, 88 FORDHAM L. REV. 129, 135–137 (providing an overview of this advertising system); ZUBOFF, *supra* note 21, at 93–97.

Maine, and it can display ads to her based on that information (perhaps advertisements for overpriced law school textbooks). This additional knowledge may allow the platform to improve its CTR to 0.05%. Finally, assume that the platform knows the user's profile information and has volumes of data on her daily engagement with the platform for the past five years, including what ads she has clicked in the past. And assume that the platform can combine this data with offline data uploaded by the advertiser.[23] Using those troves of data may allow the platform to improve its CTR to 0.1%. A CTR of 0.1% may seem small in the abstract, but the improvement from a 0.01% to a 0.1% CTR equates to an enormous increase in revenue generated per user. Spread out over millions upon millions of daily users, even miniscule improvements in the accuracy of a platform's predictions will substantially increase its revenue.[24]

This advertising-centric business model creates two problematic incentives for platforms. The first is to collect and database ever-increasing amounts of information on their users in order to improve the accuracy of the platforms' predictions. This incentive can lead to privacy intrusions when the platforms initially collect and store user information and when they subsequently use that information for ad-targeting purposes.

Indeed, platforms target advertisements to users based on sensitive information that users would often prefer to keep private. For example, a 2015 report from the Office of the Privacy Commissioner of Canada found that advertising networks displayed targeted ads about sensitive topics such as pregnancy tests, bankruptcy, divorce lawyers, and liposuction.[25] Tim Wu recounts an example of a man who began seeing targeted ads for funeral services shortly after he was diagnosed with pancreatic cancer.[26] People experiencing depression,

[23] *See, e.g.*, *Create a Customer List Custom Audience*, META BUSINESS HELP CENTER, https://www.facebook.com/business/help/170456843145568?id=2469097953376494 (last visited Mar. 3, 2023) (describing how marketers can upload a list of customer emails, phone numbers, and addresses to target ads to their existing customers on Facebook); *About Lookalike Audiences*, META BUSINESS HELP CENTER, https://www.facebook.com/business/help/164749007013531?id=401668390442328 (last visited Mar. 3, 2023) (explaining how marketers can create a lookalike audience based on a source audience's "demographics, interests and behaviors").

[24] *See, e.g.*, ZUBOFF, *supra* note 21, at 95 (quoting a Microsoft researcher's conclusion that "even a 0.1% accuracy improvement in our production would yield hundreds of millions of dollars in additional earnings").

[25] ONLINE BEHAVIOURAL ADVERTISING (OBA) FOLLOW UP RESEARCH PROJECT, OFF. OF THE PRIV. COMM'R OF CAN. (June 2015), https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2015/oba_201506/.

[26] WU, *supra* note 21, at 324.

grappling with revealing their gender identity or sexual orientation, losing their religion, and working through similar intimate challenges may see constant reminders of their struggles from marketers looking to sell a product or service online.[27] Targeted advertising "can be a particularly brutal reminder of trauma because the ads feel so personal and individualized, and because what you search for or browse online can affect the ads you see, creating a feedback loop of pain."[28]

Worse yet, platforms' ad targeting practices can create or perpetuate social inequities. Platforms can serve people wildly different ads based on what their online behaviors reveal about their incomes, education levels, zip codes, races, genders, sexual orientations, and so on.[29] Those ads can, for example, influence where a person attends college, which loan they take out to afford college, which apartment they rent during college, and which insurance company they use for renters'' insurance.[30] A lower-income military veteran residing in a majority-Black zip-code might be bombarded with ads for for-profit colleges and financial products with unfavorable terms. Change one of those attributes and the person might soon be exposed to a far more advantageous array of educational, housing, and financial options.

[27] Rae Nudson, *When Targeted Ads Feel a Little Too Targeted*, VOX (Apr. 9, 2020, 10:20 AM), https://www.vox.com/the-goods/2020/4/9/21204425/targeted-ads-fertility-eating-disorder-coronavirus (providing examples including ads for menstrual products, fertility products, ads related to sexuality or gender, and more).

[28] *Id.*

[29] Eli Pariser recounts an example of two friends who searched for "BP" in 2010, shortly after the BP Deepwater Horizon oil spill. One friend saw "investment information about BP," as well as a "promotional ad from BP." The other friend saw news about the oil spill. The friends experienced these wildly different search results despite both being "educated, white, left-leaning women who live in the Northeast." As Pariser puts it, "[i]f the results were that different for these two progressive East Coast women, imagine how different they would be for my friends and, say, an elderly Republican in Texas . . . ." ELI PARISER, THE FILTER BUBBLE: WHAT THE INTERNET IS HIDING FROM YOU 2–3 (2011).

[30] *See, e.g.*, Sandra Wachter, *Affinity Profiling and Discrimination by Association in Online Behavioral Advertising*, 35 BERKELEY TECH. L.J. 367, 375–80 (2020) (describing how online behavioral advertising can lead to a variety of discriminatory outcomes); Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 131 YALE L.J. F. 907, 921–27 (2022) (describing, in relevant part, the discriminatory exclusion and discriminatory predation that African Americans experience as a result of online ad targeting); FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? 10 (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf ("Participants raised concerns that when big data is used to target ads, particularly for financial products, low-income consumers who may otherwise be eligible for better offers may never receive them.").

The second problematic incentive created by platforms' ad-centric business models is the persistent need to drive engagement with users; that is, to maximize the amount of time users spend interacting with platforms. Increased engagement allows platforms to display more ads to their users and to collect more information about their users, thus improving the accuracy of platforms' targeting programs.[31] This need to foster constant user engagement informs several aspects of platform creation and management. For example, nearly all platforms now feature "endless scrolls," where instead of hitting the end of a page and having to click to a next page to see more content, new content (and new advertisements, of course) continuously loads as the users scrolls down.[32] Even details that seem benign, like the color of a notification badge, may be selected with careful attention to driving user engagement.[33] It is easy to get sucked in—to get addicted—to social media when platforms are tailor-made for that purpose.[34]

Compounding these addictive design features, platforms use complex algorithms to curate content for users with the aim of maximizing engagement.[35] And what content tends to keep users' eyes on their screens? As Professor Kyle Langvardt explains, "it seems that the most reliable engagement drivers are messages that stimulate feelings of outrage and group identification."[36] Shocking content, controversial content, and conspiracy theories may thus enjoy preferred status over less viscerally exciting but more socially beneficial content.[37]

[31] *See* Langvardt, *supra* note 22, at 134, 137 (explaining that social media companies are "obsess[ed]" with "driving engagement" and identifying increased ad volume and accuracy as the reasons behind this obsession).

[32] *Id.* at 142–46 (discussing the "endless scroll" design feature).

[33] *Id.* at 142.

[34] *See id.* at 141–51 (describing how platform design features can lead to problematic habit-forming behaviors and other social challenges); *see also* Alan Z. Rozenshtein, *Silicon Valley's Speech: Technology Giants and the Deregulatory First Amendment*, 1 J. FREE SPEECH L. 337, 356 (2021) (discussing Langvardt's research).

[35] *See* ZUBOFF, *supra* note 21, at 457–59; Raymond Brescia, *Privacy's "Three Mile Island" and the Need to Protect Political Privacy in Private-Law Contexts*, 48 FLA. ST. U. L. REV. 973, 989–90 (2021).

[36] Langvardt, *supra* note 22, at 149.

[37] *See id.* (noting that "[m]any recommendation algorithms . . . have been shown repeatedly to send users along a 'radicalizing' path"); Julie Cohen, *Tailoring Election Regulation: The Platform is the Frame*, 4 GEO. L. TECH. REV. 641, 657 (2020) ("[Platforms] amplify socially networked flows in ways that elicit conditioned, automatic, and tribal responses because that is the approach that most reliably enriches their shareholders and venture investors.").

B. Beyond Commerce: Problems with Political Ad Targeting on Platforms

As anyone who follows elections in the United States knows, the appeal of advertising on internet platforms is not limited to corporations looking to sell a product. Campaigns looking to sell a politician, and politicians looking to sell a message, can leverage such advertising to spread their gospel. In the four years from 2014 to 2018, online political advertising increased an estimated 2,539 percent, from $71 million (1% of overall political ad spending) to $1.9 billion (22% of overall spending).[38] That trend continued into the 2020 election, when online political advertising became even more important due to campaigns' limited abilities to engage voters in person during the early stages of the COVID-19 pandemic. Overall, online political advertising exceeded $2.8 billion in 2020.[39] In the Presidential election alone, digital advertising exceeded $430 million from April to November of 2020 (24.3% of overall ad spending in the Presidential general election).[40]

This extraordinary growth of online political advertising carries some democratic benefits. The low price tag of online advertising lowers the barriers of entry for candidates and political groups to reach the electorate when compared to traditional advertising mediums like television, print, and radio.[41] Candidates and groups can use platforms' targeting tools to reach (and expand) their intended audiences in an incredibly efficient manner. And online advertising allows users to engage with candidates in a way that traditional media advertising does not: one click and the user can instantly access a wealth of information about the candidate's background and campaign platform.

But the explosion in online political advertising poses severe challenges for our democracy as well. First, as the 2016 U.S. Presidential election infamously revealed, nefarious actors can weaponize platforms' microtargeting tools toward anti-

[38] Megan Janetsky, *Low Transparency, Low Regulation Online Political Ads Skyrocket*, OPEN SECRETS (Mar. 7, 2018, 4:29 PM), https://www.opensecrets.org/news/2018/03/low-transparency-low-regulation-online-political-ads-skyrocket/.

[39] *See 2020 Political Digital Advertising Report*, TECH FOR CAMPAIGNS, https://www.techforcampaigns.org/impact/2020-political-digital-advertising-report (last visited Mar. 3, 2023).

[40] Wesleyan Media Project, *Political Ads in 2020: Fast and Furious* (Mar. 23, 2021), https://mediaproject.wesleyan.edu/2020-summary-032321/.

[41] *See, e.g.*, TECH FOR CAMPAIGNS, *supra* note 39 (explaining the cost advantages digital advertising carry for smaller and newer campaigns).

democratic ends.[42] Second, political ad microtargeting creates harmful filter bubbles.[43] Filter bubbles, in turn, prevent speakers with opposing or different viewpoints from presenting effective counter-speech,[44] and they erode shared truths and shared norms that are important to sustaining democratic self-governance.[45] Third, relying on users' online behaviors and other personal information to target political ads intrudes on intellectual and political privacies that are important to maintaining a well-functioning democracy.[46]

1. Misuse by Nefarious Actors

On February 16, 2018, a grand jury impaneled as part of Special Counsel Robert Mueller's probe into Russian interference in the 2016 U.S. Presidential election returned an indictment charging a Russian government agency known as the Internet Research Agency (the "IRA"), along with several Russian persons, with conspiracy to defraud the United States, conspiracy to commit wire fraud and bank fraud, and aggravated identity theft.[47] The indictment explained how the IRA employed hundreds of individuals to create fake personas and "group pages" on social media sites in order to "create political intensity through supporting radical groups, users dissatisfied with the social and economic situation and oppositional social

[42] *See infra* Part II(B)(1).

[43] *See, e.g.*, Nunziato, *supra* note 21, at 2539–41.

[44] *See* Abby K. Wood & Ann M. Ravel, *Fool Me Once: Regulating "Fake News" and other Online Advertising*, 91 S. CAL. L. REV. 1223, 1277 (2018).

[45] *See, e.g.*, Nunziato, *supra* note 21, at 2544 ("[P]olitical ads disseminated via traditional media are subject to broad exposure and broad public scrutiny—which are necessary for the truth-facilitating features of the marketplace of ideas mechanisms to function. Microtargeted ads, on the other hand . . . are not similarly subject to broad exposure or broad public scrutiny."); Cohen, *supra* note 37, at 652 ("Voter microtargeting efforts move and are designed to move on the collective level, nurturing rumor and innuendo, hardening targeted populations in their tribal responses to real and perceived differences, and frustrating the sorts of efforts toward rapprochement on which theories about republican self-government rely.") and 657–58 (describing platforms as posing a threat to an "anti-factionalism" and "anti-authoritarian" interests); Christopher S. Elmendorf & Abby K. Wood, *Elite Political Ignorance: Law, Data, and the Representation of (Mis)Perceived Electorates*, 52 U.C. DAVIS L. REV. 571, 606–08 (2018).

[46] *See* Ira Rubenstein, *Voter Privacy in the Age of Big Data*, 2014 WISC. L. REV. 861, 904–07 (2014) (explaining the importance of intellectual and political privacy to democratic participation and summarizing literature on the subject); *see also* Neil Richards, *Intellectual Privacy*, 87 TEX. L. REV. 387 (2008). Cohen, *supra* note 37, at 658, describing an "anti-manipulation" interest that can be thought of as overlapping with intellectual and political privacy concerns.

[47] *See* Indictment, United States v. Internet Research Agency LLC, *et al.*, 1:18-cr-00032-DLF (Doc. 1) (Feb. 16, 2018).

movements."[48] It used these fake personas and groups to sow divisions in American society and to support President Trump's campaign.[49]

One of the most comprehensive accounts of the IRA's social media operation comes from a study based on data from Facebook and Twitter provided to the authors by the Senate Select Committee on Intelligence.[50] On Facebook, the IRA created dozens of fake group pages, designed to look like they were formed and managed by U.S. persons, centered around distinct social groups or hot-button political issues. The most active groups included those designed to appeal to patriotism and southern culture ("Being Patriotic," "Heart of Texas," and "South United"), minorities ("Blacktivist," "United Muslims of America," "LGBT United," "BM (Black Matters)," and "Brown Power"), religious Christians ("Army of Jesus"), and persons with anti-immigrant views ("Stop A.I. (All Invaders))."[51]

The IRA then ran thousands of advertising campaigns to attract Americans to join these groups. By using the same advertising tools that businesses use to target consumers, the IRA was able to microtarget its campaigns to the specific segments of the U.S. population it wanted to reach. The Howard *et al.* study examined these thousands of advertising campaigns and divided them into categories based on the IRA's targeting decisions. For instance, an ad campaign targeting people interested in "'Mexico,' 'Chicano rap' and 'Hispanidad'" would "suggest the IRA was intending to target Latin American . . . users."[52] Some of the most common targets of the IRA's ads were people interested in "African American Politics and Culture," "Black Identity and Nationalism," "Conservative Politics and Culture," "Latin American Culture," "Social Justice," "Pro-gun Politics,"

[48] *Id.* ¶ 10(a), 33, 34.

[49] *Id.* ¶ 6 (noting the "strategic goal to sow discord in the U.S. political system" and the goal of "supporting the presidential campaign of then-candidate Donald J. Trump").

[50] Philip N. Howard *et al.*, *The IRA, Social Media and Political Polarization in the United States, 2012-2018* (2019), https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1004&context=senatedocs; *see also* Ellen L. Weintraub & Carlos A. Valdivia, *Strike and Share: Combatting Foreign Influence Campaigns on Social Media*, 16 OHIO ST. TECH. L.J. 702–06 (2020) (summarizing Russia's use of social media to influence the 2016 U.S. Presidential election and to sow division in the United States).

[51] Philip N. Howard *et al.*, *The IRA, Social Media and Political Polarization in the United States, 2012-2018* (2019), https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1004&context=senatedocs.

[52] *Id.* at 18.

"LGBT Rights & Social Liberalism," "Immigration," "Muslim American Politics and Culture," and "Veterans & Policing."[53]

By microtargeting these segments of the population, the IRA was able to grow membership in its group pages. This allowed the IRA to use organic posts to spread "a wide range of disinformation and junk news" to large, segmented audiences.[54] The Agency targeted the audiences it built through its politically conservative group pages with content designed to "energize conservatives around Trump's campaign."[55] And it targeted its more liberal audiences with content aimed to "encourage . . . cynicism . . . in an attempt to neutralize their vote."[56]

The reach of this nefarious content was not limited to group members themselves. When a group page posts content, the content appears in the group members' news feeds. Group members can then interact with the content by "liking" it, sharing it, or commenting on it. These interactions in turn cause the content to appear in the group-member's friends' news feeds. Those friends can also interact with the post, and can join the group page, further expanding the size of the group's audience. Thus, a relatively small initial investment in political ad microtargeting to attract members to a group page can, over time, generate a massive audience. One source estimates that Russian forces spent a total of $400,000 and were able to reach about 200 million users.[57]

Russia's 2016 operation may be the most prominent instance of a nefarious actor weaponizing political ad microtargeting tools, but it does not stand alone. The same election cycle brought us the Cambridge Analytica scandal, in which data harvested from users' Facebook profiles was used by the Trump campaign (among others) for ad targeting purposes.[58] More recently, Meta has published regular reports detailing its efforts to take down coordinated inauthentic behavior ("CIB") operations that often originate in foreign nations.[59] Some of these

[53] *Id.* at 23.

[54] *Id.* at 32.

[55] *Id.*

[56] *Id.*

[57] Ian Vanderwalker and Lawrence Nodren, *Getting Foreign Funds Out of America's Elections*, BRENNAN CTR. JUST. (Apr. 9, 2018), https://www.brennancenter.org/our-work/policy-solutions/getting-foreign-funds-out-americas-elections.

[58] *See e.g.*, Sam Meredith, *Facebook-Cambridge Analytica: A timeline of the data hijacking scandal*, CNBC (Apr. 10, 2018), https://www.cnbc.com/2018/04/10/facebook-cambridge-analytica-a-timeline-of-the-data-hijacking-scandal.html.

[59] *See* Meta, *Coordinated Inauthentic Behavior Explained* (Dec. 6, 2018), https://about.fb.com/news/tag/coordinated-inauthentic-behavior/ (explaining

operations have been aimed at establishing an American social media presence to use as a weapon in future elections.[60] And the techniques employed by foreign actors are becoming more sophisticated. The IRA, for example, has reportedly tried to "exploit a hole in Facebook's ban on foreigners buying political ads" by "paying American users to hand over personal pages and setting up offshore bank accounts to cover their financial tracks."[61] Simply put, the problem of nefarious actors leveraging social media platforms—especially the platforms' ad targeting tools—to interfere with U.S. democracy is an ongoing national security threat.[62]

2. Filter Bubbles, Counter Speech, & Shared Truths

Filter bubbles form when a platform serves content to users based on the platform's predictions about the users' preferences.[63] Most major platforms operate this way since their

coordinated inauthentic behavior, detailing Facebook's efforts to combat the practice, and compiling reports).

[60] *See, e.g.*, *Facebook removes 203 accounts for foreign interference from Russia*, REUTERS (Mar. 12, 2020), https://www.reuters.com/article/facebook-content/facebook-removes-203-accounts-for-foreign-interference-from-russia-idUKL4N2B55BG (noting that the removed accounts "frequently posted U.S. news and attempted to add audience through topics that included black history, black excellence and fashion, celebrity gossip and LGBTQ issues"); Shannon Bond, *Facebook Removes Chinese Accounts Posting About Foreign Policy, 2020 Election*, NPR (Sept. 22, 2020), https://www.npr.org/2020/09/22/915778396/facebook-removes-chinese-network-posting-about-foreign-policy-2020-election; Steven Overly, *Facebook removes foreign accounts targeting U.S. election*, POLITICO (Oct. 27, 2020), https://www.politico.com/news/2020/10/27/facebook-removes-foreign-accounts-targeting-election-432843. In a related, domestic problem, right-wing militia groups utilized Facebook's ad targeting tools in 2020 to promote their extremist messages. Ryan Mac & Caroline Haskins, *Facebook Has Been Profiting From Boogaloo Ads Promoting Civil War and Unrest*, BUZZFEEDNEWS (June 30, 2020), https://www.buzzfeednews.com/article/ryanmac/facebook-instagram-profit-boogaloo-ads.

[61] Matthew Rosenberg *et al.*, *'Chaos is the Point': Russian Hackers and Trolls Grow Stealthier in 2020*, N.Y. TIMES (Jan. 10, 2020), https://www.nytimes.com/2020/01/10/us/politics/russia-hacking-disinformation-election.html.

[62] *See* Joint Statement from DOJ, DOD, DHS, DNI, FBI, NSA, and CISA on Ensuring Security of 2020 Elections (Nov. 5, 2019), https://www.fbi.gov/news/press-releases/press-releases/joint-statement-from-doj-dod-dhs-dni-fbi-nsa-and-cisa-on-ensuring-security-of-2020-elections (identifying Russia, China, and Iran as potentially using social media campaigns to "influence voter perceptions"); Jessica Watson, *Microtargeting as Information Warfare*, 6 CYBER DEFENSE REV. 63 (2021) (framing political ad microtargeting as a national security threat).

[63] *See* PARISER, *supra* note 29, at 9 (introducing the term "filter bubble"); *see also* CASS SUNSTEIN, *REPUBLIC.COM* (2001); CASS R. SUNSTEIN, #REPUBLIC: DIVIDED DEMOCRACY IN THE AGE OF SOCIAL MEDIA (2017); Wood & Ravel, *supra* note 44, at 1236–37.

business models revolve around predicting user preferences and displaying content and advertisements that match those preferences.[64] Rather than being exposed to a diverse set of viewpoints, users thus primarily see information that aligns with their predicted preferences.

Filter bubbles existed long before the internet and long before platforms across the internet chose to hyper-personalize users' information flows. People chose to read certain newspapers, watch certain news stations, or follow certain bloggers, while disregarding others. But today's filter bubbles are meaningfully different. As Eli Pariser explained in introducing the concept of a filter bubble more than a decade ago, modern filter bubbles are: (a) personalized to the individual rather than a large group of people with a common interest; (b) invisible to users, who often don't know that a platform is personalizing content for them, let alone *why* the platform is showing them particular content; and (c) virtually unavoidable for internet users.[65]

Microtargeted political ads contribute to platforms' filter bubble effect as one of at least three primary and inter-related causes. The first cause involves user self-selection. When a social media user chooses to join groups or follow other users that all have the same (or similar) ideological viewpoints, the user will primarily see content that reflects that ideological viewpoint. The second cause involves the algorithms that platforms employ to serve content to users. As discussed *supra*, platforms have a tremendous financial incentive to show users content with which the user wants to engage. This generally means that algorithms serve content "that reinforces [users'] tribal inclinations—especially content that triggers outrage or affords opportunities to signal affiliation."[66] Once the algorithm has predicted your tribe, the connections you make and the content you see will likely deepen your tribal affinity.

Political ad microtargeting intensifies the filter-bubbling effect caused by these other two factors. Campaigns can target platforms' already-filtered user bases with near-personalized messaging, catering the content of political ads to users' predicted preferences and then refining that targeted messaging

[64] *See, e.g.*, Tim Wu, *Is the First Amendment Obsolete*, 117 MICH. L. REV. 547, 555–56 (describing the link between platforms' business models and the rise of filter bubbles).

[65] PARISER, *supra* note 29, at 9–10.

[66] Cohen, *supra* note 37, at 647.

through A/B testing.[67] Layered upon the organic political content that the platform curates just for them, users are bombarded during election season with political advertising curated based on their predicted preferences.[68]

Filter bubbles offend well-established free speech values. This is so in at least two respects. First, filter bubbles undermine speakers' ability to present counter-speech. The Supreme Court has based its First Amendment jurisprudence in large part upon the belief that speech must be protected to facilitate a healthy marketplace of ideas.[69] The notion of a marketplace of ideas presupposes that listeners will be subject to multiple, competing viewpoints, with the best speech rising to the proverbial top.[70] However, when the information ecosystem devolves into a series of filter bubbles, listeners hear less and less counter-speech (and more and more affirming speech), creating a structural market flaw.

The negative effect on counter-speech caused by filter bubbles is especially pronounced in the context of political ad microtargeting.[71] Since campaigns can easily target advertisements containing unique messages to a group of only hundreds of voters—among electorates that often range in the tens-of-millions—it is nearly impossible for opposing speakers to counter the targeted advertisements' claims.[72] The task is

[67] *See e.g.*, Elmendorf & Wood, *supra* note 45, at 607 (noting that online advertising allows campaigns to "run thousands of variations of an advertisement every day, using A/B testing to discover the messages that maximize clicks").

[68] It is worth pausing to appreciate how these latter two causes of filter bubbles obfuscate what I previously termed the "self-selection" cause of filter bubbles. After a user makes an initial content selection on a platform, the platform's predictive algorithm will influence the user's subsequent selections by displaying content and advertisements with which it believes the user will engage based on the user's initial selection. Indeed, the predictive algorithm may even influence the initial selection. If the platform already has information about the user—say, through the initial registration process—it can suggest content to the user before the user even makes a selection.

[69] *See, e.g.*, Nunziato, *supra* note 21, at 2492–93 (explaining the marketplace of ideas theory); G. Michael Parsons, *Fighting for Attention: Democracy, Free Speech, and the Marketplace of Ideas*, 104 MINN. L. REV. 2157, 2162–80 (2020) (describing and critiquing the Court's marketplace of ideas framework).

[70] Nunziato, *supra* note 21, at 2492–93.

[71] *See, e.g.*, *id.* at 2537–40 (describing the effect political ad microtargeting has on counter-speech); PARISER, *supra* note 29, at 155–56 (predicting, in 2011, that political ad microtargeting would make counter-speech nearly impossible).

[72] *See* Peter Kafka, *Facebook's Political Ad Problem, Explained by an Expert*, VOX (Dec. 10, 2019, 8:00 AM), https://www.vox.com/recode/2019/12/10/20996869/facebook-political-ads-targeting-alex-stamos-interview-open-sourced (quoting former Facebook executive Alex Stamos as stating that "[i]f you allow people to show an ad to just 100 folks,

particularly insurmountable when we consider the effects on a large scale, rather than in the context of countering a single ad. At scale, political advertisers segment the population in different ways for their numerous ad campaigns. Any particular user is included or excluded from each audience segment based on any of hundreds of different data points about the user. Each user is then subject to a unique slate of political ads based on their inclusion or exclusion in each of these thousands (upon thousands) of audience segments. It is as if the advertiser is "whispering millions of different [political] messages into zillions of different ears for maximum effect and with minimum scrutiny."[73] With a minimal ability for counter-speakers to scrutinize and contest these advertisements within earshot of the relevant audiences, the false or otherwise noxious messaging in the advertisements can more easily become accepted truths to the viewers. That accepted truth can then be reinforced through other information viewed in the filter bubble, be it through advertisements or organic content displayed based on an algorithm's (tribalistically inclined) predictions. Rinse and repeat for every platform user in the electorate.

The second subsidiary problem caused by filter bubbles is the dissolution of shared truths and norms. Jurists and First Amendment scholars have long identified the search for truth as one of the core values of preserving free speech.[74] Establishing shared truths is, in turn, essential to maintaining a well-functioning democracy: Through a healthy speech market, shared truths and norms can emerge and may then form the foundation for reaching democratic agreement on matters of public import.[75]

Filter bubbles impinge the public's ability to establish common beliefs about both truths and norms. "Broadcast-

and then you run tens of thousands of ads, then it makes it extremely difficult for your political opponent and the print media to call you out").

[73] Nunziato, *supra* note 21, at 2544 (quoting Kara Swisher, *Google Changed Its Political Ad Policy. Will Facebook Be Next?*, N.Y. TIMES (Nov. 22, 2019)).

[74] *See, e.g.*, Thomas Emerson, *Toward a General Theory of the First Amendment*, 72 YALE L.J. 877, 881 (1963) ("[F]reedom of expression is . . . to begin with, the best process for advancing knowledge and discovering truth."); Whitney v. California, 274 U.S. 357, 375 (1927) (Brandeis, J., concurring) ("[The framers] believed that freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth . . . .").

[75] *See, e.g.*, Emerson, *supra* note 74, at 882 (explaining how free speech is imperative for societies to "reach common decisions that will meet the needs and aspirations of its members"); PARISER, *supra* note 29, at 5, 50, 164 (discussing the importance of shared truths and norms to maintaining a healthy democracy, in the context of filter bubbles).

television advertisements that appeal to widely shared values" are increasingly being "supplanted by micro-targeted, social-media-conveyed appeals to the prejudices and predilections of individual recipients."[76] As a result, "[d]emocracy-sustaining norms of mutual respect and accommodation may be at risk, to say nothing of shared understandings about facts."[77] And by "hardening targeted populations in their tribal responses to real and perceived differences," microtargeting "frustrate[es] the sorts of efforts toward rapprochement on which theories about republican self-government rely."[78] Simply put, the more fragmented our political information environment becomes, the more difficult it becomes to agree on what our politics should be.

3. Intellectual & Political Privacy

Finally, the microtargeting of political advertisements threatens the intellectual and political privacies needed for self-government to properly function. These values—like the presentment of counter-speech and the establishment of shared truths—also find roots in First Amendment jurisprudence. Professor Neil Richards explains this in his 2008 article, *Intellectual Privacy*:

> Intellectual privacy is the ability, whether protected by law or social circumstances, to develop ideas and beliefs away from the unwanted gaze or interference of others. Surveillance or interference can warp the integrity of our freedom of thought and can skew the way we think, with clear repercussions for the content of our subsequent speech or writing. The ability to freely make up our minds and to develop new ideas thus depends upon a substantial measure of intellectual privacy. In this way, intellectual privacy is a cornerstone of meaningful First Amendment liberties.[79]

[76] Elmendorf & Wood, *supra* note 45, at 575; *see also* Ellen P. Goodman, *Digital Fidelity and Friction*, 21 NEV. L.J. 623, 626 (2021) (critiquing platforms' structures as producing "a noisy information environment that is inhospitable to the production of shared truths and the trust necessary for self-government").

[77] Elmendorf & Wood, *supra* note 45, at 606.

[78] Cohen, *supra* note 37, at 652.

[79] Richards, *supra* note 46, at 389.

Political privacy, for present purposes, may be thought of as an important genus of intellectual privacy. It is the ability to develop ideas and beliefs *about political matters* away from the unwanted gaze or interference of others. Because intellectual and political privacy are foundational to a well-functioning democratic process, the need to safeguard this aspect of privacy expands beyond the prevention of individual harms (with which privacy protections are usually associated). Rather, the democratic dimension to intellectual and political privacy "marks a shift from privacy as an individual value to privacy as a social or public value that matters to individuals in their role as citizens."[80]

The microtargeting of political ads threatens the public value of intellectual and political privacy. As Ira Rubenstein explained, while writing toward the inception of political ad microtargeting in 2014, "if the First Amendment protects the right to read anonymously, then this protection also must extend to seeking information online and refusing to share information about one's tastes, preferences, interests, and beliefs, which is exactly the type of information that campaigns obtain through . . . profiling."[81] Thus, voters should be

> entitled to seek and gain access to online political information without having to disclose their political leanings or suffer the chilling effect of pervasive monitoring and tracking of their every thought and belief. In the face of such pervasive monitoring and tracking of voters' online behavior by every campaign web site and every ad-funded online newspaper, magazine, blog, and most other sources of political information, surely the First Amendment must protect voters' freedom of thought. If not, an essential precondition of democracy will be undermined.[82]

The threat to intellectual and political privacy posed by political ad microtargeting has only grown more severe as

[80] Rubenstein, *supra* note 46, at 904; *see also* Sofia Grafanaki, *Autonomy Challenges in the Age of Big Data*, 27 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 803, 818–19, 855 (2017) (discussing the importance of intellectual privacy to individual autonomy in a free society).

[81] Rubenstein, *supra* note 46 at 907.

[82] *Id.* (building upon Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996)).

campaigns have refined their targeting practices by using platforms' increasingly sophisticated tools. Now, "every election cycle will come with new challenges and will force us to rethink the legality of campaigning practices" to ensure that sophisticated political ad targeting techniques do not "compromis[e] values that are necessary preconditions for democratic life, such as political privacy."[83]

***

In sum, platforms operate based on an advertising-centric business model that incentivizes them to collect as much information about users as possible. Platforms then use these troves of information to display users' content that maximizes the users' engagement with the platform and also to display ads with which users are most likely to engage. The platforms' never-ending quest for more information and more engagement leads to a series of broad-based problems: privacy invasions, discriminatory outcomes, and internet addiction.

More acutely, the personal information that platforms amass allows them to microtarget ads to minute segments of the population. Commercial actors have deployed these microtargeting tools with great success, but when platforms allow the tools to be used for political advertising purposes, significant dangers emerge. First, the tools can be exploited by nefarious actors who aim to undermine liberal democracy. Second, the practice of microtargeting political ads exacerbates platforms' filter-bubbling effects, making the presentment of counter-speech exceedingly difficult and reducing opportunities to establish shared truths and norms. And third, the practice poses harms to intellectual and political privacies that are important to sustaining a well-functioning democracy.

Legal scholars have long appreciated the risks that platforms' business models pose to liberal democracy, and they are increasingly focusing on the more specific harms caused by political ad microtargeting.[84] But while we are in the midst of grappling with that problem, the technology behind the problem is changing. And it is changing in a way that, I fear, will greatly exacerbate the existing problems identified in Part II.

[83] Grafanaki, *supra* note 80, at 860.

[84] See, for example, the sources cited throughout Part II(B).

III. POLITICAL ADVERTISEMENTS IN VIRTUAL REALITY

A. VR Technologies and Biometric Monitoring

The experience of being in a VR environment is, in a word, breathtaking. One source describes such environments as "replac[ing] users' real-world surroundings convincingly enough that they are able to suspend disbelief and fully engage with the created environment."[85] That was certainly my experience—suspended disbelief—as I soaked in the views from the summit of Mount Everest in my first experience using the Oculus VR headset a few years ago.[86] Or take a friend's account of playing the VR version of ADR1FT, a game in which the user plays an astronaut trying to survive the destruction of a space station:[87] My friend described the physical sensation of breathlessness that he felt when the astronaut began to run out of oxygen in space, and the sensation of helplessness he experienced when the astronaut eventually died.[88] Professors Lemley and Volokh recount a similar story to describe just how real VR environments feel. People using the Oculus Rift VR Headset were reluctant to walk across a virtual plank, high in the virtual air. Some people refused outright, others panicked and removed their headsets, while the brave souls who stepped off the plank "invariably lean[ed] forward as they [took] that one step, because their body [was] signaling them that they [were] falling."[89] That example is from 2013. ADR1FT was released in 2016. The technology was amazing then; it is better now; and it will only get better moving forward.

So how does it work? How are these technologies able to create the sensation of reality in users who nonetheless know they are in a virtual environment? The magic increasingly involves biometric monitoring.

[85] Ivy Wigmore, *Definition: Immersive Virtual Reality (Immersive VR)*, TECHTARGET.COM (Aug. 2016), https://www.techtarget.com/whatis/definition/immersive-virtual-reality-immersive-VR.

[86] *See Everest VR*, METAQUEST, https://www.oculus.com/experiences/rift/1043021355789504/ (last visited July 25, 2022).

[87] ADR1FT, IGN, https://www.ign.com/games/adr1ft (last visited July 25, 2022).

[88] Indeed, a review by the tech company Nvidia describes the "stifling sense of claustrophobia, and frustrating lack of self-control," as well as the "bewildering and heart pounding exercise" that users experience when playing ADR1FT. ADR1FT Review, NVIDIA, https://www.nvidia.com/en-us/geforce/news/gfecnt/adr1ft-fight-for-survival-in-space-in-the-gripping-vr-experience-now-on-oculus-rift/ (last visited July 25, 2022).

[89] Mark A. Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality*, 166 U. PA. L. REV. 1051, 1064 (2018).

Users access VR environments by donning a head-mounted display ("HMD"). When a user puts on the HMD, the device displays a video feed that encompasses the user's entire range of vision (the user cannot see the "real world"). To make the video feed realistic enough to create the sensation of *realness*—to get the user to "suspend disbelief"—HMDs track, at a minimum, the user's head and body position and adjust the video depending on where the user is looking and moving.[90]

For example, Meta's Oculus Quest 2 HMD uses a tracking technology known as six degrees of freedom.[91] The technology tracks the user's movement in six ways: "forward, backward, up, down, side-to-side, and the tilt angle of the user's head."[92] The video feed from the HMD seamlessly adjusts based on the user's positioning, just as a person's field of vision naturally adjusts when they turn their head or move their body. Quest 2 also tracks users' hand movements through cameras positioned on the HMD, allowing users to interact with their virtual environments by pointing, pinching, and scrolling.[93]

Some sophisticated VR technologies currently available on the market go even further. HTC's line of VIVE products include full-body tracking,[94] a facial tracker,[95] and an eye tracker.[96] VIVE's facial tracker sells for a mere $129 and can "[r]ead intentions and emotions in real-time" by tracking "38 blend shapes across the lips, jaw, teeth, tongue, cheeks, and chin."[97] Users can pair the facial tracker with VIVE Pro Eye

[90] *See* Heller, *supra* note 13, at 13–16 (describing how VR technologies function).

[91] *Meta Quest 2 and Meta Quest Headset Tracking*, META, https://store.facebook.com/help/quest/articles/headsets-and-accessories/using-your-headset/turn-off-tracking/ (last visited July 25, 2022).

[92] Heller, *supra* note 13, at 14.

[93] *Getting Started with Hand Tracking on Meta Quest 2 and Meta Quest*, META, https://store.facebook.com/help/quest/articles/headsets-and-accessories/controllers-and-hand-tracking/hand-tracking-quest-2/ (last visited July 25, 2022).

[94] *Introducing VIVE Tracker (3.0)*, VIVE, https://www.vive.com/us/accessory/tracker3/ (last visited Apr. 12, 2023) ("Use multiple trackers and recreate your real-life movements in VR with precise accuracy."); *see also* Ben Lang, *Meta Says Full-body Tracking Probably Not Viable with Inside-out Headsets*, ROAD TO VR (Feb. 16, 2022), https://www.roadtovr.com/meta-quest-2-full-body-tracking-fbt-not-viable-quest-2/ (explaining the different between "inside-out tracking," where the tracking camera is on the HMD and tracking is mostly limited to head and hand positions, and "outside-in tracking," where an external camera(s) allows for full body tracking).

[95] *VIVE Facial Tracker*, VIVE, https://www.vive.com/us/accessory/facial-tracker/ (last visited July 25, 2022).

[96] *Pro Eye*, VIVE, https://www.vive.com/us/product/vive-pro-eye/overview/ (last visited July 25, 2022).

[97] *VIVE Facial Tracker*, *supra* note 95.

(which, VIVE boasts, can "[t]rack and interpret eye movements")[98] for "a whole-face tracking experience."[99] Finally, in the months leading up to this article's publication, Meta and Pico both released HMDs with built-in eye tracking and face tracking capabilities.[100]

As noted above, some of these biometric monitoring technologies are integral to VR functionality. If an HMD did not track users' head positions, it could not create the immersive, virtual environment that the user purchased the HMD to access. Facial recognition trackers may soon be needed for VR avatars to mimic users' facial movements as they interact with others in VR environments. And eye tracking has several beneficial uses in VR, from reducing hardware costs and energy requirements by "provid[ing] high resolution only where you are looking," to improving users' experience as they navigate virtual spaces.[101]

Other biometric monitoring technologies will integrate into VR in varying degrees, depending upon what use-cases for VR emerge. To take a fun example, full body tracking is a practical necessity for the sub-culture of break-dancers who use VR technologies to compete in virtual breakdancing competitions.[102] Widely used wearable devices like FitBits and Apple Watches can monitor your stress level and heart rate,[103] and with Meta's marketing focus on Quest's health and exercise applications, such monitors seem like prime candidates for long-term VR integration.[104] Louis Rosenberg predicts that biometric

[98] *Pro Eye*, *supra* note 96.

[99] *VIVE Facial Tracker*, *supra* note 95; *see also* Heller, *supra* note 13, at 29 (explaining how facial tracking can be used to indicate users' emotional responses of "anger, surprise, fear, joy, sadness, contempt, and disgust").

[100] *See Meta Quest Pro*, META, https://www.meta.com/help/quest/articles/headsets-and-accessories/quest-pro/index-quest-pro/#name2 (last visited Feb. 2, 2023) (describing the HMD's ability to capture facial expressions and track eye movement); *see Pico 4 Enterprise*, PICO, https://www.picoxr.com/global/products/pico4e (last visited Feb. 2, 2023).

[101] Avi Bar-Zeev, *The Eyes Are the Prize: Eye-Tracking Technology Is Advertising's Holy Grail*, VICE (May 28, 2019, 10:48 AM), https://www.vice.com/en/article/bj9ygv/the-eyes-are-the-prize-eye-tracking-technology-is-advertisings-holy-grail.

[102] *See* Ben Lang, *The Future is Now: Live Breakdance Battles in VR Are Connecting People Across the Globe*, ROAD TO VR (Jan. 18, 2021), https://www.roadtovr.com/vr-dance-battle-vrchat-breakdance/.

[103] *See Apple Watch Series 7*, APPLE, https://www.apple.com/apple-watch-series-7 (last visited July 26, 2022); *FitBit Sense*, FITBIT, https://www.fitbit.com/global/us/products/smartwatches/sense (last visited July 26, 2022).

[104] *See, e.g.*, *Fitness is Fun on Meta Quest*, META, https://www.meta.com/quest/experiences/fitness/ (last visited Sept. 28, 2022).

monitoring in the metaverse will also include vocal inflections, vital signs, gait, posture, pace, and certain hand movements.[105]

B. Biometric Psychography and VR Advertising

As more types of biometric monitoring become necessary (or useful) to VR technologies' functionality, the potential secondary use of biometric data for targeted advertising in VR becomes more alarming. In perhaps the most well-developed account of VR technologies in legal scholarship, Brittan Heller describes exactly how biometric monitoring used in VR technologies can lead to exploitative targeted marketing opportunities.[106] As she explains, VR companies can use biometric tracking to compile dossiers on how a user's body reacts to external stimuli in VR environments over time.[107] The companies can then use the insights gained from these dossiers—combined with other personal and behavioral information—to predict and shape the user's behavior, including, most significantly, selecting which advertising messages to display to the user.[108]

To provide a straightforward example, Heller asks the reader to imagine they are playing a VR racing game.

> You look down the line of cars and settle on a sleek, cherry red convertible. As you run your virtual hands along its virtual hood, your body responds with signs of excitement—your heart rate increases, your skin moistens, and your pupils dilate. The VR hardware records these involuntary biological reactions . . . . [R]ed convertibles soon begin popping up in your virtual and online spaces, along with advertisements for new car insurance and reminders to renew your driver's license. User information from the racing game has been sold to companies, advertising agencies, and government agencies. It is used to target experiences, services, or products that you are prone to like, and to predict your consumer preferences and personal opinions . . . . Playing a

[105] Rosenberg, *supra* note 4, at 7.

[106] Heller, *supra* note 13; *see also* Bar-Zeev, *supra* note 101 (cataloguing the various uses of eye tracking technologies in VR advertising).

[107] Heller, *supra* note 13, at 27–28.

[108] *Id.* at 6, 27–28.

> VR racing game is like hitting a "like button" on steroids.[109]

Your involuntary biological reaction to the red convertible would become another data point in a comprehensive dossier that maps your physical responses to external stimuli in the environment—just as every like, upvote, comment, click, and friend connection becomes data for marketers today. Over time, VR companies would have thousands upon thousands of data points about your involuntary biological reactions to external stimuli and what those reactions reveal about your preferences. Heller terms this practice *biometric psychography*: "[T]he gathering and use of biological data, paired with the stimuli that caused a biological reaction, to determine users' preferences, likes, and dislikes."[110]

The biometric monitoring devices that are (or may soon be) incorporated into VR technologies can be used to make ads more persuasive—and manipulative—in other ways as well. For example, VR expert Avi Bar-Zeev explains how companies can use eye tracking in VR to conduct sophisticated A/B testing on what captures users' attention.[111] By tracking where users are looking, VR companies can display different permutations of products, logos, people, etc. in users' periphery. They can then track which permutations lead people to shift their gaze toward the object or person being displayed—does the blue car garner more attention, or the red one?[112] Bar-Zeev also notes how VR companies could use their knowledge of what your face looks like to create advertisements featuring people who resemble you. As he puts it, "facial similarity works to build trust and relationships," and marketers can use that trust to increase the likelihood users will interact with their brands.[113]

For simplicity, I will collectively refer to biometric psychography and other uses of biometric data to craft advertisements, like those identified by Bar-Zeev, as "biometric

[109] *Id.* at 3.

[110] *Id.* at 6.

[111] *See* Avi Bar-Zeev, *XR Can Read Your Mind, but not the Way You Think*, MEDIUM (Sept. 9, 2022), https://medium.com/predict/xr-can-read-your-mind-but-not-the-way-you-think-29069a4b2b63; *see also* Bar-Zeev, *supra* note 101.

[112] *Id.*

[113] *Id.*; *see also* Rosenberg, *supra* note 4, at 6 ("[T]he manner in which these simulated people appear will be crafted for maximum persuasion—their gender, hair color, eye color, clothing style, voice and mannerisms—will be custom generated by algorithms that predict which sets of features are most likely to influence the targeted user based on previous interactions and behaviors.").

targeting." Biometric targeting in VR advertising sounds like a distant theoretical development in some future dystopian society; something out of Minority Report or a Black Mirror episode, to invoke a couple of over-used pop culture references. But it is not.

First, VR advertising is already happening. In September 2022, the metaverse-like gaming platform Roblox (discussed in further detail below) announced its plans to launch a VR advertising platform in 2023.[114] Roblox intends to include virtual billboards, "portal" ads that will transport users into branded spaces, and native ads where companies can pay to brand various objects in VR worlds, like a basketball in a sports game.[115]

Second, companies are already using biometric monitoring to craft marketing strategies.[116] Many of those monitors can already be integrated with VR technologies, and some of them *must* be integrated for the technologies to function.[117] To take one example, companies are beginning to

[114] Peter Adams, *Roblox's Ad Expansion Plans Include 3D Portals to Branded Experiences*, MARKETINGDIVE (Sept. 12, 2022), https://www.marketingdive.com/news/roblox-immersive-ads-metaverse-Robux-Gen-Alpha/631622/.

[115] Patrick Kulp, *Roblox is Testing Dynamic Billboards in the Metaverse With New Ad Platform*, ADWEEK (Sept. 9, 2022), https://www.adweek.com/commerce/roblox-testing-dynamic-billboards-in-the-metaverse-new-ad-platform.

[116] Indeed, there is a whole cottage industry of marketing agencies that offer companies the ability to measure consumers' biological reactions to products and messaging. *See, e.g.*, Jessica Davies, *The BBC is Using Facial Recognition to Measure if Native Ads Work*, DIGIDAY (Jan. 21, 2016), https://digiday.com/media/bbc-facial-recognition-native-advertising/; *Affective Introduces New Functionality to Enhance Media Analytics Insight*, AFFECTIVA, https://www.affectiva.com/news-item/affectiva-introduces-new-functionality-to-enhance-media-analytics-insight/ (last visited July 28, 2022); Sophie Charara, *Hollywood is Tracking Heart Pounding Movie Scenes With Wearable Tech*, WAREABLE (Jan. 18, 2016), https://www.wareable.com/wearable-tech/heart-racing-bear-scenes-the-revenant-2186. Further, retailers are already deploying biometric ad targeting in the brick-and-mortar context. *See, e.g.*, Kiely Kuligowski, *Facial Recognition Advertising: The New Way to Target Ads to Consumers*, BUSINESS NEWS DAILY (June 29, 2022), https://www.businessnewsdaily.com/15213-walgreens-facial-recognition.html (discussing Walgreen's use of facial recognition technology to target ads on refrigerator doors in their stores); *Smart Vending Machine Scans Your Face to Serve Up Snacks*, NBC NEWS (Mar. 5, 2014), https://www.nbcnews.com/tech/innovation/smart-vending-machine-scans-your-face-serve-snacks-n45546 (discussing use of facial recognition technology in vending machines to target products based on the consumer's age and gender); Drew Bates, *SMB Innovation Lab: Face Recognition with in-Store Analytics*, SAP (May 18, 2018), https://blogs.sap.com/2018/05/18/smb-innovation-lab-face-recognition-with-in-store-analytics/ (marketing an app that pairs with facial recognition technologies for retailers).

[117] *See* Heller, *supra* note 13, at 29 ("[D]ata that enables biometric psychography *must* be captured for immersive technology to function, which means this field will likely grow as immersive tech expands.").

pair VR technologies with electroencephalography ("EEG") in controlled research environments. EEG is a non-invasive method of measuring electrical waves generated by the brain that can be performed by using a head cap affixed with electrodes.[118] EEG has several medical applications[119] but is also used for consumer research by tracking the electrical activity in subjects' brains when they are shown external stimuli, such as an advertisement.[120] A recent review of market research studies performed using EEG revealed widespread application, with EEG being used to study product characteristics and preferences; gender and cultural differences among consumers; pricing considerations; various advertising techniques; and brand identity.[121] The review also showed that an increasing number of market research studies are combining EEG with other biometric devices, such as eye tracking, electromyography ("EMG") and galvanic skin response ("GSR").[122] EEG devices that can integrate with VR technologies are already available on the market.[123]

EMG, GSR, and electrocardiography ("ECG") can similarly be used to reveal consumers' physiological reactions to external stimuli, such as products or messaging. For instance, a recent market research study utilized EMG—which uses electrodes to measure the electrical activity of the subject's muscles—and an eye-tracking device to measure consumers' responses to various skin care products.[124] The researchers attached electrodes to specific facial muscles associated with smiling and frowning and then tracked how the subjects' facial expressions changed in response to different packaging, pricing, and brands.[125] Similar examples can be found in market research

[118] *Electroencephalography (EEG)*, JOHNS HOPKINS MED., https://www.hopkinsmedicine.org/health/treatment-tests-and-therapies/electroencephalogram-eeg (last visited Sept. 28, 2022); *see* Heller, *supra* note 13, at 28–29.

[119] *E.g.*, JOHNS HOPKINS MED., *supra* note 118.

[120] *See, e.g.*, Andrea Bazzani et al., *Is EEG Suitable for Marketing Research? A Systematic Review*, FRONTIERS IN NEUROSCIENCE 1, 2–6 (Dec. 2020) (analyzing 113 market research studies performed using EEG since 2000).

[121] *See generally id.*

[122] *Id.* at 6–7.

[123] *See DSI VR300*, WEARABLE SENSING, https://wearablesensing.com/products/vr300/ (last visited Feb. 25, 2022) (advertising a research-grade EEG system that is designed for "VR integration" and that "interfaces seamlessly with the HTC-Vive VR headset").

[124] Gabriel Levrini & Mirela Jeffman dos Santos, M., *The Influence of Price on Purchase Intentions: Comparative Study Between Cognitive, Sensory, and Neurophysiological Experiments*, BEHAV. SCI. 2021 1, 1 (Feb. 2021).

[125] *Id* at 6–8.

literature for GSR (which can reveal the intensity of subjects' emotional states by measuring their sweat gland activity) and ECG (which measures heart rate).[126]

Third, VR advertising platforms, like their 2D internet counterparts discussed above, will have a tremendous financial incentive to improve the accuracy of their predictions about users.[127] And, crucially, these companies will not need to literally read users' minds to improve the effectiveness of their advertising platforms—they don't need to wait until head-to-toe (or brain-to-heart) monitoring is a part of the VR experience (if we ever get that far) to deploy biometric targeting. Since even miniscule improvements in advertising effectiveness translate to huge revenue gains,[128] all biometric targeting needs to deliver is a slightly more accurate prediction about user behavior than companies would be able to garner without it.

The pieces of the puzzle are in place; all that is left is for VR companies to put the pieces together . . . and they already are. In recent years, Meta has filed numerous patent applications for technology the company could use to build its Metaverse's advertising platform.[129] The patent applications contemplate a bidding system, similar to Meta's current ad auction system, in which marketers could bid to sponsor content in its Metaverse.[130] As part of the bidding system, sponsored content would be scored based on how likely the particular user is to interact with it, which would in turn be determined based on "characteristics associated with the user."[131] And which characteristics would best reveal the user's affinity for the sponsored item? The

[126] *See, e.g.*, Jung Ha-Brookshire & Gargi Bhaduri, *Disheartened Consumers: Impact of Malevolent Apparel Business Practices on Consumer's Heartrates, Perceived Trust, and Purchase Intention*, 1 FASHION & TEXTILES 1, 1, 5 (2014) (using ECG to monitor subjects' reactions to malevolent messaging about apparel businesses); Rafal Ohme et al., *Analysis of Neurophysiological Reactions to Advertising Stimuli by Means of EEG and Galvanic Skin Response Measures*, 2 J. OF NEUROSCIENCE, PSYCH., AND ECON. 21, 21, 24 (2009) (using GSR and other measurements to study consumers' reactions to different versions of an advertisement). *See also* Mascha van 't Wout et al., *Skin Conductance Reactivity to Standardized Virtual Reality Combat Scenes in Veterans with PTSD*, 42 APPLIED PSYCHOPHYSIOLOGY BIOFEEDBACK 209, 209 (2017) (pairing VR technologies with GSR to measure veterans' reactions to depictions of combat).

[127] *See supra* Part II(A).

[128] *See id.*

[129] *See* Hannah Murphy, *Facebook Patents Reveal How It Intends to Cash in on Metaverse*, FINANCIAL TIMES (Jan. 18, 2022), https://www.ft.com/content/76d40aac-034e-4e0b-95eb-c5d34146f647.

[130] Elinor Carmi, *Facebook Patent Shows How You May Be Exploited in the Metaverse*, TECH POLICY PRESS (Nov. 18, 2021), https://techpolicy.press/facebook-patent-shows-how-you-may-be-exploited-in-the-metaverse/.

[131] *Id.* (quoting from the patent application).

applications don't say it outright, but it's not hard to read between the lines. Indeed, a Financial Times analysis of Meta's patents concluded that the company has already "patented multiple technologies that wield users' biometric data in order to help power what the user sees" and that Meta "hopes to use tiny human expressions to create a virtual world of personalised ads."[132]

C. Translation to Political Advertising

Writing about filter bubbles in 2011, Eli Pariser posited that "the state of the art in political advertising is half a decade behind the state of the art in commercial advertising."[133] In hindsight, the use of political ad microtargeting in the 2016 election cycle makes that predicted timeframe seem eerily accurate.

If we are already seeing the seeds being planted for the commercial use of biometric data to target commercial VR advertisements then the time to start examining its political use is now.[134] In this subsection, I identify three forms that political advertising could take in VR environments. I then describe a hypothetical VR campaign rally to illustrate how the political use of biometric targeting threatens to greatly exacerbate the extant problems with microtargeted political ads identified in Part II.

1. Forms of Political Advertising in VR

I anticipate that three general methods of delivering political advertisements in VR environments will emerge, each of which could utilize biometric targeting to individualize messaging to users.

First, political advertising could be delivered through display advertising. A display ad is an ad that displays content in a way that makes it apparent to the user that what the user is seeing is in fact an ad.[135] Billboards, banner ads, pop-ups, and video commercials are generally display ads. When you are viewing content, playing a game, or entering a new space in a VR environment, you may have to view a display advertisement,

[132] Murphy, *supra* note 129.

[133] PARISER, *supra* note 29, at 154.

[134] *Cf.* Heller, *supra* note 13, at 6–7 (making the same point, three years ago, about commercial advertising in VR environments).

[135] *See, e.g.*, *Display Ads*, MAILCHIMP, https://mailchimp.com/marketing-glossary/display-ads/#Display_ads_versus_native_ads (last visited Feb. 26, 2023) (distinguishing display ads from native ads based on the latter being "less obvious" to users).

just as you currently do before watching a video on YouTube, while scrolling through your Instagram feed, and so on. Some of these display ads may be political ads.

In contrast, a native ad is an ad that is designed to appear like it is content generated by the platform, or by another user, and not by the marketer—an ad that the user is not supposed to know is an ad.[136] Native ads can take different forms. One form is a product placement, such as when your favorite TV character cracks open an ice-cold Pepsi. Product placement opportunities will be plentiful in VR environments. For example, "if a story [in a game] calls for a car, a particular sponsor's car will be introduced for the player to drive. Any object could be replaced based on hidden automatic ad auctions."[137]

Going further, native advertising can take the form of sponsor-generated content. Rather than a company sponsoring a car in a game, the company can sponsor the entire game (or show, or movie, or whatever).[138] This practice has long been common in the gaming world (sponsor-created games are known as "advergames") and in other forms of media.[139] Finally, native advertising can be conducted through paid spokespersons (commonly known as "influencers") who do not disclose that they are being paid to promote a product, service, or brand.[140] In

[136] *See, e.g.*, Note, Irina Dykhne, *Persuasive or Deceptive? Native Advertising in Political Campaigns*, 91 S. CAL. L. REV. 339, 340 (2018) (describing native ads as those that "match the editorial content of media or technology platforms"); *Native Advertising: A Guide for Businesses*, FED. TRADE COMM'N, https://www.ftc.gov/business-guidance/resources/native-advertising-guide-businesses (last visited Mar, 2, 2023) (describing native advertising as "content that bears a similarity to the news, feature articles, product reviews, entertainment, and other material that surrounds it online").

[137] Brittan Heller & Avi Bar-Zeev, *The Problems with Immersive Advertising: In AR/VR, Nobody Knows You Are an Ad*, 1 J. OF ONLINE TR. AND SAFETY 1, 6 (Oct. 2021); Kulp, *supra* note 115.

[138] Heller & Bar-Zeev, *supra* note 136, at 7 (providing the example of a Jurassic Park game).

[139] Going way back, some Atari and Nintendo games were advergames. Older millennials and Gen-Xers may remember playing Yo! Noid, which featured Domino Pizza's mascot; Cool Spot, a same about the red spot on 7-up cans; or Kool-Aid Man, an Atari game about the Kool-Aid Man. *See Yo! Noid*, MOBY GAMES, https://www.mobygames.com/game/yo-noid (last visited Jan. 25, 2023); *Cool Spot*, MOBY GAMES, https://www.mobygames.com/game/cool-spot (last visited Jan. 25, 2023); *Kool-Aid Man*, MOBY GAMES, https://www.mobygames.com/game/atari-2600/kool-aid-man (last visited Jan. 25, 2023).

[140] *See, e.g.*, Alexandra J. Roberts, *False Influencing*, 109 GEO. L.J. 81, 84–85 (2020) (describing influencer marketing and explaining how sponsored influencer messaging can "masquerade as organic buzz and peer-to-peer testimonial" when it lacks proper disclosures).

VR, these spokespersons need not even be persons; they could be AI-powered avatars.[141]

A recent complaint about Roblox submitted to the FTC by Truth in Advertising.org ("TINA.org") foreshadows the native advertising opportunities that will be available in VR environments.[142] Roblox is, in short, an early version of a metaverse, with a particular focus on gaming.[143] The gaming platform allows users to both create their own games and play games created by other users.[144] Users play the games (called "experiences" on the platform) and interact with other users through self-created avatars, which they can dress and accessorize with virtual items that they purchase with a digital currency called Robux.[145] Roblox has over 100 million monthly active users, including more than half of all American children under 16.[146] The platform is not strictly a VR environment, though some games on Roblox do take place in such environments and can be accessed with a Meta Quest or HTC Vive HMD.[147]

The TINA.org complaint highlights each of the three types of native advertising practices described above. Sponsored content appears within organic games and alongside non-sponsored content in the Roblox avatar store.[148] Roblox lists advergames alongside user-created experiences in ways that give users "no way of knowing which of these [experiences] are unsponsored authentic content and which are corporate-controlled advertisements."[149] And Roblox is replete with undisclosed avatar influencers, some of which are human-created while others are AI-generated.[150] Such native advertising opportunities will continue as VR technologies progress. As

[141] Rosenberg, *supra* note 4, at 5–6.

[142] *See* Letter from TINA.org to the F.T.C., *Deceptive Marketing on Roblox* (Apr. 19, 2022), https://truthinadvertising.org/wp-content/uploads/2022/04/4_19_22-Complaint-to-FTC-re-Roblox.pdf [hereinafter, TINA Complaint].

[143] *Id.* at 2 (describing Roblox).

[144] *Id.* at 2–3.

[145] *Id.* at 3.

[146] Taylor Lyles, *Over Half of US Kids Are Playing Roblox, and It's About to Hose Fornite-esque Virtual Parties Too*, THE VERGE (July 21, 2020, 7:16 PM), https://www.theverge.com/2020/7/21/21333431/roblox-over-half-of-us-kids-playing-virtual-parties-fortnite.

[147] *See* Roblox, *Roblox VR*, https://en.help.roblox.com/hc/en-us/articles/208260046-Roblox-VR (last visited Aug. 1, 2022) (providing instructions for how to use Roblox with Vive or Oculus).

[148] *See* TINA Complaint, *supra* note 142, at 11–13.

[149] *Id.* at 5.

[150] *Id.* at 13–18.

Brittan Heller and Avi Bar-Zeev put it, one problem with immersive advertising will be that "nobody knows you are an ad."[151]

It is not difficult to imagine how political campaigns can leverage these native advertising opportunities.[152] Indeed, a candidates' likeness or logo can be immersed into users' VR environments just like any other product. Maybe a candidate's campaign shirt will appear as an option in your virtual closet. You might see a candidate's avatar playing alongside you in a game, waving to you while you walk down a virtual street, or singing along to your favorite jam at a virtual concert. Perhaps you'll start playing a game about a post-apocalyptic future and learn that society collapsed after candidate Jones was elected. And that avatar over there—the one holding the "Smith 2032" banner—is that a regular citizen, a paid influencer, or an AI-generated bot?[153]

While display and native advertising are familiar categories, VR technologies unlock the potential for a new, third, form of political messaging, which I call *immersive electioneering environments*. An immersive electioneering environment is, in short, a VR event space dedicated to campaigning. Just as concerts and similar events are already taking place in such spaces,[154] candidates may soon hold campaign rallies, speeches, and more personal meet-and-greets in VR environments. Importantly, campaigns could pay platforms or developers to custom tailor these virtual event spaces, much like an event planner would set up a gymnasium for a big speech.[155] Except

[151] Heller & Bar-Zeev, *supra* note 137, at 1.

[152] Campaigns began advertising in video games as early as 2008. *See* Dykhne, *supra* note 136, at 363 (describing then-candidate Obama's use of advertising in video games).

[153] *Cf.* Anastasia Goodwin et al., *Social Media Influencers and the 2020 U.S. Election: Paying 'Regular People' for Digital Campaign Communication*, CTR. FOR MEDIA ENGAGEMENT (Oct. 2020), https://mediaengagement.org/wp-content/uploads/2020/10/Social-Media-Influencers-and-the-2020-U.S.-Election-1.pdf (examining the practice of paying social media influencers to promote political content).

[154] *See, e.g.*, Adi Robertson, *Warner Music Group is Launching a Metaverse Concert Hall Where You Can Pay to Be Its Neighbor*, THE VERGE (Jan. 27, 2022, 11:01 AM), https://www.theverge.com/2022/1/27/22904382/warner-music-group-the-sandbox-virtual-real-estate-sale-concert-venue; Bernard Marr, *The World of Metaverse Entertainment: Concerts, Theme Parks, And Movies*, FORBES (July 27, 2022, 2:07 AM), https://www.forbes.com/sites/bernardmarr/2022/07/27/the-world-of-metaverse-entertainment-concerts-theme-parks-and-movies/?sh=5dba7b806531.

[155] There is already a whole industry of companies who specialize in planning events in immersive reality environments. *See Metaverse Events: Immersive Experience for Event Attendees*, EVENTDEX (Dec. 16, 2021), https://www.eventdex.com/blog/metaverse-

these virtual architects won't just be arranging virtual furniture, they'll be constructing environments that collect information about all who enter.

The key aspect of my theorized immersive electioneering environments is that they will enable campaigns to access a wealth of information about users who enter the environments. It will be like when websites collect visitors' information via cookies, or when third-party apps pull data about users from social media platforms, only to a more extreme degree. When a person enters an immersive electioneering environment, the campaign could, in theory, gain access to any of the aforementioned types of (biometric and other) personal information that VR technologies enable it to collect. That could range from basic demographic information, to the user's social connections, to the user's biometric psychographic profile.

While less familiar to readers than display and native advertising, the creation of immersive electioneering environments is less far-off than it may seem at first blush. Sophisticated political campaigns have long been fueled by troves of voter data, often collected and put to use through cutting-edge technologies.[156] VR companies are already making huge investments in virtual concerts and other events.[157] Companies that specialize in virtual event planning already highlight their ability to collect and analyze attendees' data.[158] And prominent politicians in the U.S. have been experimenting with VR technologies and early metaverses since at least 2015.[159]

events-immersive-experience/; *All the Ingredients to Host a Successful Virtual or Hybrid Event*, vFAIRS, https://www.vfairs.com/features/ (last visited Aug. 1, 2022); *Xyrisid Virtual Trade Show*, XYRIS INTERACTIVE DESIGN, INC., https://xyris.ca/metaverse/ (last visited Aug. 1, 2022); *About Wave*, WAVE, https://wavexr.com/about/ (last visited Aug. 1, 2022).

[156] *See, e.g.*, Rubenstein, *supra* note 80 at 862–66 (describing the role of big data in U.S. elections).

[157] *E.g.*, *Announcing Venues in Horizon Worlds*, META: META QUEST BLOG (June 6, 2022), https://www.oculus.com/blog/announcing-venues-in-horizon-worlds/ (announcing integration of venues into Meta's Horizon Worlds metaverse, which will allow Horizon Worlds users to seamlessly access events, concerts, or "even host [their] own meet-up").

[158] *See vFAIRS*, *Features*, http://www.vfairs.com/features (last visited Aug. 1, 2022) (highlighting the customer's ability to "get deep audience insights with our event reporting" and to "view user behaviour" to "see exactly what went well and what didn't").

[159] *See, e.g.*, Alaa Elassar, *Joe Biden Has His Own Island on 'Animal Crossing' Where You Can Learn About His Campaign*, CNN (Oct. 18, 2020 6:53 PM), https://www.cnn.com/2020/10/18/business/biden-animal-crossing-island-trnd/index.html; Scott Hayden, *2016 Presidential Candidate Bernie Sanders Makes 360 Video Appearance*, ROAD TO VR (July 23, 2015), https://www.roadtovr.com/2016-presidential-candidate-bernie-sanders-makes-360-video-appearance/; Paul Tassi,

***

There is little inherently wrong with political advertising in VR environments. Such messaging, if properly regulated, could allow voters to connect with candidates in a more meaningful, interpersonal manner than current technology allows. Indeed, politicians have been using new technologies to better achieve that type of connection for just about as long as there have been politicians.[160]

The problem, of course, lies in how VR technologies may allow campaigns to target their messaging.[161] By supplementing the types of information that social media platforms currently collect about users with data derived from biometric monitoring, campaigns could individualize political messaging—through display ads, native ads, and immersive electioneering environments—with heretofore unseen precision.[162]

2. The Dystopian Extreme: "Rodriguez 2036"

Allow me to provide an example of how the combination of biometric targeting, VR, and associated technologies could lead to unprecedented levels of individualization in political advertising.

AOC Just Gave Her First Ever Commencement Address—In 'Animal Crossing', FORBES (May 9, 2020, 8:43 AM), https://www.forbes.com/sites/paultassi/2020/05/09/aoc-just-gave-her-first-ever-commencement-address--in-animal-crossing/?sh=e90d9477d4c0; Cathy Hackl, *Andrew Yang Turns Himself Into An Avatar And Campaigns In The Metaverse*, FORBES (Jun. 11, 2021, 10:32 AM), https://www.forbes.com/sites/cathyhackl/2021/06/11/andrew-yang-turns-himself-into-an-avatar-and-campaigns-in-the-metaverse/?sh=18eb6e862460.

[160] President Franklin D. Roosevelt's fireside chats and President Kennedy's live televised press conferences are prime historical examples. *See* Margaret Biser, *The Fireside Chats: Roosevelt's Radio Talks*, THE WHITE HOUSE HIST. ASS'N (Aug. 19, 2016), https://www.whitehousehistory.org/the-fireside-chats-roosevelts-radio-talks (discussing FDR's use of radio to connect with the public); *John K. Kennedy and the Press*, JFK PRESIDENTIAL LIBRARY AND MUSEUM, https://www.jfklibrary.org/learn/about-jfk/jfk-in-history/john-f-kennedy-and-the-press (last visited Aug. 2, 2022) (discussing JFK's use of live televised press conferences to connect with the public).

[161] Similarly, one of the most prominent critics of online political advertising, Ellen Weintraub, has argued that online political advertising *sans* microtargeting is a benign practice. *See* Weintraub & Valdivia, *supra* note 50, at 716; Ellen L. Weintraub, *Don't Abolish Political Ads on Social Media. Stop Microtargeting*, WASH. POST (Nov. 1, 2019), https://www.washingtonpost.com/opinions/2019/11/01/dont-abolish-political-ads-social-media-stop-microtargeting/.

[162] *See supra* Part II(A) (discussing social media ad targeting); Part III(A) (discussing biometric psychography).

It is 2036. There is a closely contested congressional race in your district; you've seen the display ads in VR, online, and on your neighbors' lawns. You've also seen people in VR donning the candidates' paraphernalia, some of whom have approached you to discuss their preferred candidate. Through these interactions, you learn about a VR campaign rally for one of the candidates, Rodriguez, and you decide to attend. The campaign announces that there will be three components to the rally: a video montage of Rodriguez on the campaign trail; a series of speeches capped by a keynote address from Rodriguez; and an interpersonal meet and greet with Rodriguez's avatar. You and thousands of other users pre-register for the rally and then head into the virtual venue that has been custom built for this event.

By the time you have registered and walked into the event, the campaign already knows the precise composition of the crowd—and not just the demographic mix. When you and everyone else registered for the rally, the platform made troves of data about registrants available to the campaign, including users' online behaviors and information derived from their biometric psychographic profile. The campaign knows how members of the crowd have reacted to various campaign ads in the past; what issues they care most about; what traits they find most favorable in leaders; and so on. And, once the crowd floods into the venue, the campaign has access to the crowd's real-time (aggregate and individualized) biometric data. That data allows the campaign to read the crowd's mood, determine how carefully the crowd is paying attention, and conduct sophisticated A/B testing for speakers and messages.

The rally begins. The display on your HMD fades to black. Suddenly you hear the sounds of silverware clanking, drinks being poured, and children's voices getting louder all around you. Your display lights back up and you are sitting at Rodriguez's breakfast table, like a member of the family. You watch as Rodriguez sends her kids to school and then hits the campaign trail. You walk with Rodriguez from door to door, watching her talk to voters about the day's issues. Then you are back at Rodriguez's dinner table, joining her family in a brief prayer before their evening meal. The montage concludes with an inspiring message, and the speeches are set to begin.

You look around at the crowd and are pleased at the people you see—a few, even, are familiar faces from your social circle. Then the warm-up speakers begin. A single parent who went to school with Rodriguez. A community activist who marched with Rodriguez in civil rights demonstrations. A fellow congressperson who works with Rodriguez day in and day out. You learn from these speeches that Rodriguez is intelligent and caring, that she is not afraid to stand up for what is right, and that she's willing to reach across the aisle. By the time it's Rodriguez's turn to speak, your impression is already favorable. She steps to the virtual podium wearing a navy blue suit, a "Peace in Ukraine" pin, and yellow and blue earrings to match the pin. As she speaks, her campaign displays a series of infographics and other visual aids that support her talking points. Her speech is impactful; the crowd cheers her off; and you are swept away into a more intimate setting with an avatar of Rodriguez.

It's your local coffee shop. The avatar is sitting across the table with a steaming hot latte in front of her. It looks so real—the avatar, the latte, all of it. You suspend disbelief and begin engaging in conversation with Rodriguez. You learn more about her family, where she stands on the issues, and even her favorite shows and podcasts. She asks you questions too, and you answer as candidly as if you were chatting with a friend.

Much of what you just experienced was individualized content, tailored to you based in part on your biometric psychography. The display and native advertising you saw in the lead-up to the rally was adjusted to your preferences. The video montage was compiled from a wider selection of video clips; you experienced the family and voter interactions that your profile suggested you would find most appealing. Your crowd placement was dictated based on the positive physiological reactions you previously displayed when interacting with the same or similar people in the metaverse—that's why you saw those aesthetically pleasing faces. You heard the three opening speakers to whom your profile suggested you would react most favorably. Rodriguez's clothes, her pin, her earrings, and the infographics behind her were all tailored to your liking. You didn't notice, but a segment of her speech was actually delivered by a deep-fake avatar (like the one you met at the coffee shop) who discussed Rodriguez's position on the issue about which you are most passionate. The setting and the content of the meet and greet was all customized for you too. Everyone else, of course, experienced the rally differently.

3. Paring (Partially) Back

Let us pull back from the Rodriguez 2036 rally. Even if targeted political advertising in VR environments never reaches this dystopian level of individualization, it is easy to see how campaigns could soon recreate elements of it. For example, campaigns could use aggregate biometric information (along with other data) about crowd makeup to segment virtual crowds into different spaces with different speakers. They could alter infographics and other content based on what users' biometric psychography reveals about their preferences. The content of display and native political advertising could change based on a user's biometric psychography just as it could for commercial products. And as with consumer research, biometric monitoring could be used to test, refine, and target candidate messaging.

Moreover, prominent political campaigns are already experimenting with deepfake versions of candidates. In early 2022, South Korean Presidential candidate Yoon Suk Yeol's campaign developed a digital version of Yoon, known as AI Yoon, using deepfake technology.[163] To the human eye, AI Yoon was indistinguishable from the real Yoon.[164] South Koreans could visit wikiyoon.com and submit questions to AI Yoon, who would respond with "salty language and meme-ready quips" drafted by campaign staffers.[165] The campaign's goal was to use AI Yoon to make the real Yoon more likeable, especially to younger voters.[166] It worked, at least anecdotally. One 23-year-old South Korean reported that the real Yoon was "dull," but the virtual version was "more likable and relatable."[167] The voter planned to cast his ballot for Yoon.[168] Seven million other people visited wikiyoon.com in the run-up to South Korea's election,[169] which Yoon won by less than a percentage point.[170]

[163] Timothy W. Martin & Dasl Yoon, *Campaigns Hope Avatars Show Human Side of Candidates*, WALL ST. J., (Mar. 8, 2022) (describing AI Yoon and how the campaign built and utilized the virtual candidate).

[164] *Id.*; *see also* WION, *Deepfake of South Korea's presidential candidate AI Yoon ahead of election*, YOUTUBE (Feb. 19, 2022), https://www.youtube.com/watch?v=yIUTvPOXkk8 (showing a news report that includes a video of AI Yoon).

[165] *Deepfake democracy: South Korean candidate goes virtual for votes*, FRANCE 24 (Feb. 14, 2022), https://www.france24.com/en/live-news/20220214-deepfake-democracy-south-korean-candidate-goes-virtual-for-votes.

[166] Martin & Yoon, *supra* note 163.

[167] *Id.*

[168] *Id.*

[169] *Deepfake democracy: South Korean candidate goes virtual for votes*, *supra* note 165.

[170] Choe Sang-Hun, *Yoon Suk-yeol, South Korean Conservative Leader, Wins Presidency*, N.Y. TIMES (Mar. 9, 2022),

AI Yoon is the first iteration of an "AI candidate," but he is unlikely to be the last. Recreate him in a VR environment and select which content to show voters based on some set of the voters' personal information, and the basic elements of what I have described above are in place.

***

What will happen to the extant problems with political ad microtargeting when this next generation of targeting techniques comes online in VR: How much damage could a nefarious political actor do with biometric targeting techniques, or by gaining access to the underlying user data (say, through a "Cambridge Analytica-type mass violation of user trust")?[171] How much more impenetrable will biometric targeting, when layered on top of existing political ad targeting tools, make each of our filter bubbles? And how much more difficult will it be for users to seek out political information without the fear that they are being surveilled as they do?

More importantly, what can we do about it?

IV. THE FIRST AMENDMENT MINEFIELD

The most straightforward way to prevent biometric targeting from exacerbating extant problems with political ad microtargeting would seemingly be for governments to restrict its use in VR political advertising. However, such restrictions would face a major impediment in the United States: the First Amendment.[172] Under the Supreme Court's prevailing jurisprudence, as expressed most clearly in *Sorrell v. IMS Health*, restrictions on speakers' use of data to craft speech appear to enjoy the same level of protection as speech itself.[173] Indeed, there is a long-running debate about whether and when restrictions on data flows cause First Amendment speech concerns, with one group of thinkers asserting that restrictions on data flows (typically enacted in the name of privacy) often

https://www.nytimes.com/2022/03/09/world/asia/south-korea-election-yoon-suk-yeol.html.

[171] Heller, *supra* note 13, at 33 (warning that unregulated sharing of immersive reality user data with developers will leave companies vulnerable to such breaches).

[172] U.S. CONST. amend. I; *see also* Cohen, *supra* note 37, at 641 ("[A]lthough one might wonder whether the data-driven, algorithmic activities that enable and invite [electoral] manipulation ought to count as protected speech at all, the Court's emerging jurisprudence about the baseline coverage of constitutional protection for speech seems poised to sweep many such information processing activities within the First Amendment's ambit.").

[173] 564 U.S. 552 (2011).

violate the Speech Clause, and another group taking the position that such restrictions ordinarily do not implicate free speech concerns.[174] That debate has recently spilled over to the biometric information context.[175] Given that a restriction on using biometric targeting for political advertising would implicate this debate about data flows *and* affect political speech considered to be at the Speech Clause's epicenter,[176] it would be certain to draw ire from skeptical jurists and scholars.

In this Section, I unpack how several aspects of the expansive, libertarian, view of the Speech Clause championed by the Supreme Court and others will hamper the government's ability to restrict political ad targeting in VR environments.[177] In subsection (IV)(A), I argue that *content-neutral* restrictions on biometric targeting will prove politically difficult, and that even if enacted, they face significant uncertainty under current Speech Clause doctrine. In subsection (IV)(B), I address *content-based* restrictions that prohibit targeting techniques as to political advertising. I argue that the Court would likely invalidate any such restriction, repeating mistakes it has made in analogous campaign finance cases.

A. Content-Neutral Restrictions (Under the Libertarian First Amendment)

The government could pass a law restricting the use of biometric targeting on a content-neutral basis. That is to say, the government could eschew a restriction on the biometric targeting of *political* speech in favor of a restriction on the use of biometric targeting for *any* speech. A content-neutral restriction could, for example, take the form of a consent requirement for companies

[174] *See generally, e.g.*, Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049 (2000); Neil Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005); Jane Bambauer, *Is Data Speech?*, 66 STAN. L. REV. 57 (2014).

[175] *Compare* Brief for First Amend. Clinic at Duke Law and Professors of Law Eugene Volokh and Jane Bambauer as Amici Curiae Supporting Defendant's Motion to Dismiss, Am. C.L. Union v. Clearview AI, Inc. 2020-CH-043553, (Ill. Cir. Ct. Cook Cnty. 2020) *with* Brief for Law Professors as Amicus Curiae Opposing to Defendant's Motion to Dismiss, Am. C.L. Union v. Clearview AI, Inc. 2020-CH-043553, (Ill. Cir. Ct. Cook Cnty. 2020).

[176] *See, e.g.*, McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 346 (1995) (describing political speech as being at "the core of the protection afforded by the First Amendment").

[177] Given the scope of this Article, my First Amendment analysis focuses on biometric targeting; however, most of the analysis applies with equal force to laws that would restrict other political ad microtargeting techniques.

to collect, use, or share the relevant data. Or rather than a process-based restriction (where companies are allowed to use the data so long as they follow a specified process, like obtaining user consent), the government could ban the use of biometric targeting altogether.[178] A total ban would be consistent with laws or proposed laws that prohibit manipulative commercial advertising practices, such as the FTC's truth in advertising rules.[179]

A content-neutral approach to preventing biometric targeting would be ideal. From a policy perspective, the problems attendant to that targeting practice may be most pronounced in the political advertising context, but they are by no means exclusive to that context.[180] The government should restrict the use of biometric targeting in commercial and other settings as well. From a doctrinal perspective, content-neutral speech restrictions avoid the application of strict scrutiny. A reviewing court would instead apply the more lenient standard of review associated with ordinary time, place, and manner speech restrictions. Such content-neutral laws must be "narrowly tailored to serve a significant governmental interest, and [must] . . . leave open ample alternative channels for communication of the information."[181]

A content-neutral approach to restricting biometric psychography would, nonetheless, carry several complications. As a threshold matter, the government may not be able to muster the political support necessary to pass such a law. If successfully deployed, biometric targeting will prove to be incredibly lucrative for companies that participate in the VR advertising ecosystem. Improving the accuracy of ad targeting means

[178] Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020) (advocating for a U.S. privacy regime centered around substantive restrictions on data processing, rather than just procedural restrictions like notice and choice).

[179] *See Truth in Advertising*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/topics/truth-advertising (last visited Aug. 9, 2022). As of this writing, the FTC is in the process of updating its guidance document on digital advertising and has sought public input on whether and how it should address "microtargeted advertisements," and "issues that have arisen with respect to advertising that appears in virtual reality or the metaverse." *FTC Staff Requests Information Regarding Digital Advertising Business Guidance Publication*, FED. TRADE COMM'N, https://www.ftc.gov/system/files/ftc_gov/pdf/Digital%20Advertising%20Business%20Guidance%20Request%20for%20Information.pdf.

[180] Heller, *supra* note 13, at 37 (proposing changes in law to protect against the commercial use of biometric psychography).

[181] McCullen v. Coakley, 573 U.S. 464, 477 (2014). "Narrow tailoring" in the content-neutral test is a less exacting inquiry than in the content-based, strict scrutiny context. *See id.* at 486.

billions in additional revenues for the companies that own the advertising platforms, not to mention the service providers who facilitate advertising on those platforms and the companies who advertise products on the platforms.[182] Given the money to be made, laws that have the effect of restricting the commercial use of biometric targeting are likely to face intense political opposition. At a minimum, industry will push for such laws to contain less effectual opt-outs—as some state privacy regimes currently have for targeted advertising—rather than opt-ins or total prohibitions.[183]

Even if the government manages to pass a general restriction on the use of biometric psychography, lawmakers will need to take care to ensure that the law is *actually* content-neutral—a task that may be easier said than done. The Supreme Court has taken a hard line on what counts as a content-based speech restriction.[184] In cases like *Reed v. Town of Gilbert* and *Barr v. American Association of Political Consultants*, the Court has made clear that *any* law that treats one type of content differently from another type of content constitutes a content-based restriction on speech that is subject to strict scrutiny.[185] Thus, seemingly benign distinctions in laws regulating speech can render the law unconstitutional. In *Reed*, the Court applied strict scrutiny and invalidated a town's sign code because the code distinguished between different types of signs (e.g., temporary wayfinding signs versus political signs) and "impose[d] more stringent restrictions" on some types of signs than others.[186] Similarly, in *Barr*, the Court determined that the Telephone Consumer Protection Act ("TCPA") was a content-based speech restriction after Congress added an exception to the law's prohibition on the

[182] *See supra* Part II(A) (describing how minor improvements in the accuracy of platforms' predictions about user behavior lead to substantial revenue increases).

[183] *See, e.g.*, Va. Code Ann. § 59.1-577(A)(5) (2023) (providing a right to opt-out from targeted advertising); Bennett Cyphers et al., *Tech Lobbyists Are Pushing Bad Privacy Bills. Washington State Can, and Must, Do Better*, EFF (Mar. 6, 2020), https://www.eff.org/deeplinks/2020/03/tech-lobbyists-are-pushing-bad-privacy-bills-washington-state-can-and-must-do (highlighting the lobbying campaign to support "milquetoast privacy bills that will give the impression of regulation without changing the surveillance business model").

[184] *See, e.g.*, Parsons, *supra* note 69, at 2241 (noting the Court's "overly broad approach to identifying content-based laws").

[185] Reed v. Town of Gilbert, 576 U.S. 155, 163–64 (2015) (declaring that even "subtle" content distinctions that "defin[e] regulated speech by its function or purpose" are subject to strict scrutiny); Barr v. Am. Ass'n of Pol. Consultants, 140 S. Ct. 2335, 2346–47 (2020) (explaining that all content-based speech restrictions are subject to strict scrutiny).

[186] *Reed*, 576 U.S. at 159.

use of robocalls (when calling cellphones) for companies trying to collect government-backed debt.[187] As the Court explained, the presence of that exception meant that a person calling to solicit money for a political candidate could not use robocall technology while a person calling to collect government-backed debt could.[188] The law treated the caller differently based on the content of their speech.

Furthermore, laws that are facially content-neutral may nonetheless be treated as content-based and subjected to strict scrutiny in some circumstances. If a facially neutral law cannot be "justified without reference to the content of the regulated speech," or if the government adopted the law because it disagrees with the message the speech conveys, the law must satisfy strict scrutiny.[189] And facially content-neutral laws that draw distinctions based on the identity of the speaker may likewise be subject to strict scrutiny.[190]

As a result of the Supreme Court's (a) broad understanding of what constitutes a content-based speech restriction and (b) its steadfastness in subjecting *all* content-based restrictions to strict scrutiny, litigants have strong incentives to frame seemingly content-neutral laws as being content-based. Recent litigation involving facial recognition technology company Clearview AI provides a particularly germane example. In the case, plaintiffs sued Clearview AI for having "captured, used, and stored their biometric identifiers without first obtaining the written release" required by Illinois' Biometric Information Privacy Act ("BIPA").[191] BIPA, in relevant part, prohibits the collection of biometric identifiers or biometric information without first obtaining the subject's informed consent.[192] While this prohibition appears to be content-neutral, the Duke Law First Amendment Clinic's amicus brief framed BIPA as a content-based speech restriction that must be subjected to strict scrutiny. As the Clinic put it:

[187] *Barr*, 140 S. Ct. at 2343.

[188] *Id.* at 2346. The Court resolved the case by severing the restriction for government-backed debt collections, rendering the law content neutral. *Id.* at 2343–44.

[189] *Reed*, 576 U.S. at 164 (quoting Ward v. Rock Against Racism, 491 U.S. 781, 791 (1989) (internal citation omitted)).

[190] *Barr*, 140 S. Ct. at 2347 (explaining how speaker-based distinctions sometimes "reflect[] a content preference") (citation omitted).

[191] Am. C.I. Union v. Clearview AI, Inc., 2020-CH-04353, at *2 (Ill. Cir. Ct. Cook Cnty. Aug. 27, 2021) (Memorandum Opinion and Order denying Defendant's motion to dismiss) (internal quotation marks and citation omitted).

[192] *See* 740 Ill. Comp. Stat. 14/15(b) (2022).

> BIPA explicitly prohibits faceprints of human faces, but not of any other type of face; Clearview can produce faceprints from pictures of cats without any legal impediment, but nonconsensual faceprints generated from pictures of human Illinois residents are restricted. Thus, the restriction of the law turns on the content of the faceprint—whether it refers to a human subject.[193]

Although the Illinois state circuit court judge disagreed with amici's position (correctly, in my view),[194] the appointment of more libertarian-minded judges during the Trump era may well give amici (and like-minded thinkers) friendlier audiences in future cases.

Consider the consequence of combining the Court's approach to content-based speech restrictions with the Court's reasoning in *Sorrell v. IMS Health* that restrictions on data used to craft speech are treated like restrictions on the speech itself.[195] The apparent result would be that any data protection law that creates distinctions between different types of data (which is to say, virtually every data protection law) would be treated as a content-based speech restriction, provided that the data could be used to facilitate speech.[196] Where the affected speech is commercial advertising, courts would subject the law to the less demanding standard of review applicable to such speech.[197] However, where the affected speech does not fit within that narrow category, the data protection law would have to survive the more stringent, strict scrutiny, standard of review.[198] Under

[193] Brief for First Amend. Clinic at Duke Law and Professors of Law Eugene Volokh and Jane Bambauer as Amici Curiae Supporting Defendant's Motion to Dismiss at 8, Am. C.L. Union v. Clearview AI, Inc. 2020-CH-04353 (Ill. Cir. Ct. Cook Cnty. Dec. 3, 2020).

[194] Am. C.I. Union v. Clearview AI, Inc., 2020-CH-04353, at *2 (Ill. Cir. Ct. Cook Cnty. Aug. 27, 2021) (Memorandum Opinion and Order denying Defendant's motion to dismiss).

[195] *See* Sorrell v. IMS Health Inc., 564 U.S. 552, 570 (2011). As aforementioned, under the Supreme Court's prevailing jurisprudence, restrictions on speakers' use of data to craft speech appear to enjoy the same level of protection as speech itself.

[196] *See, e.g.*, Ashutosh Bhagwat, *In Defense of Content Regulation*, 102 IOWA L. REV. 1427, 1444–46 (2017) (explaining how the *Sorrell* Court's reasoning, when combined with the Supreme Court's approach to identifying content-based speech restrictions, would render most privacy laws "content-based restrictions on speech").

[197] *Sorrell*, 564 U.S. at 572 (categorizing the *Central Hudson* test as a form of "heightened scrutiny"); *see* Cent. Hudson Gas & Elec. v. Pub. Serv. Comm'n, 447 U.S. 557, 566 (1980) (establishing the test for commercial speech).

[198] *See, e.g.*, Bhagwat, *supra* note 196, at 1444–46.

this line of reasoning, a seemingly content-neutral restriction designed to prohibit the use of biometric targeting would need to survive strict scrutiny if challenged by someone wanting to target political messaging using that technique.

Surviving strict scrutiny is always a tall task, but it is especially so when the case involves political speech. The Supreme Court has repeatedly declared that political speech is the core of what the First Amendment protects.[199] It thus views laws that restrict political speech with tremendous skepticism, even when the proffered government interest is weighty.[200] This leads to a particularly vexing First Amendment problem that Professor Ryan Calo has highlighted in his embryonic work, *Digital Market Manipulation*.[201] Candidates and causes that "leverage individual biases to make their campaigns more effective" pose "an arguably greater threat to autonomy" than commercial actors that adopt similar techniques.[202] However, restrictions on such practices "sensibly occasion more serious pushback from the First Amendment," given the importance of political speech.[203] In other words, the First Amendment provides greater protection for false or misleading *political* speech than for other forms of false or misleading speech even if such speech is comparatively more problematic.[204] Thus, if the government tries to restrict biometric targeting on the ground

[199] *E.g.*, Eu v. San Francisco Cnty. Democratic Cent. Comm., 489 U.S. 214, 223 (1989) ("[T]he First Amendment 'has its fullest and most urgent application' to speech uttered during a campaign for political office." (quoting *Monitor Patriot Co. v. Roy*, 401 U.S. 265, 272 (1971))). *See also infra* notes 210-216 and accompanying text (citing to Citizens United).

[200] Citizens United v. Fed. Election Comm'n, 558 U.S. 310, 359–61 (2010) (concluding that the government's interest in preventing corruption did not justify federal law's restrictions on corporate independent expenditures)..

[201] Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995 (2014).

[202] *Id.* at 1049.

[203] *Id.*

[204] *See* Susan B. Anthony List v. Driehaus, 814 F.3d 466, 472–76 (6th Cir. 2016) (applying strict scrutiny and striking an Ohio law that prohibited persons from disseminating known or recklessly false statements about political candidates); Commonwealth v. Lucas, 472 Mass. 387, 392 (2015) (invalidating, on state constitutional free speech grounds, a statute that criminalized certain false statements about political candidates and ballot measures); 281 Care Comm. v. Arneson, 766 F.3d 774, 784–89 (8th Cir. 2014) (applying strict scrutiny and invalidating a Minnesota law that prohibited known or reckless falsities in paid political advertising about ballot questions); *see also* United States v. Alvarez, 567 U.S. 709, 738 (2012) (Breyer, J., concurring) (applying intermediate scrutiny to a law prohibiting false claims of military valor but distinguishing speech that occurs in "political contexts"); Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, 425 U.S. 748, 771–72 (1976) ("[M]uch commercial speech is not provably false, or even wholly false, but only deceptive or misleading. We foresee no [First Amendment] obstacle to a State's dealing effectively with this problem.").

that the practice is misleading or deceptive, a reviewing court may well find that government interest to be insufficient in an as applied challenge involving political advertising.

Finally, even if a reviewing court determines that a restriction on the use of biometric targeting is content-neutral, it could conclude that the restriction does not survive the Court's test for content-neutral laws. The Tenth Circuit's reasoning in *U.S. West v. FCC*—a case involving the commercial speech doctrine—demonstrates this point.[205] There, the Tenth Circuit held that an FCC regulation requiring telecommunications customers to opt into the sharing of certain data violated the First Amendment.[206] The court reasoned that the FCC regulation failed both the government interest and narrow tailoring prongs of the *Central Hudson* commercial speech test. Regarding the former prong, the FCC asserted a generalized interest in protecting consumer privacy, which the court, essentially, found to be too wishy-washy to constitute a "substantial" government interest.[207] On the latter prong, the court found that the FCC failed to carry its burden of showing that the opt-in requirement was narrowly tailored; the FCC could have instituted an opt-out rule instead.[208] A similar mode of analysis could doom a content-neutral restriction on biometric targeting, particularly if the government fails to articulate the specific privacy harms the restriction safeguards, and fails to show that less restrictive measures would be insufficient to achieve such protection.

***

I do not mean to argue or imply that a reviewing court *should* hold that content-neutral restrictions on the use of biometric targeting violate the First Amendment. My own view is quite the opposite. Rather, I am warning that such restrictions—if enacted—will likely be challenged; that the challengers can exploit several features of current Speech Clause doctrine to paint such restrictions as unconstitutional; and that those arguments may well find receptive audiences at the highest levels of the federal judiciary. Content-neutral restrictions on the use of biometric targeting are not certain to survive the First

[205] 182 F.3d 1224 (10th Cir. 1999), *cert. denied sub. nom* Competition Pol'y Inst. v. U.S. W., Inc., 530 U.S. 1213 (2000).
[206] *Id.* at 1228.
[207] *Id.* at 1234–35.
[208] *Id.* at 1238–39.

Amendment in an as-applied challenge regarding political advertising.

B. Content-Based Restrictions (Under the Libertarian First Amendment)

If enacting a content-neutral restriction on the use of biometric targeting proves politically implausible, governments may opt to enact content-based restrictions for political advertising. Content-based restrictions on political speech pose a thorny constitutional conundrum: Political speech lies at the core of the First Amendment, yet some restrictions on political speech may be important—and even necessary—to furthering the First Amendment's role in preserving self-government.[209]

Campaign finance restrictions serve as the primary illustration of this tension. U.S. governments have long placed restrictions on campaign contributions and on certain expenditures because the influence of concentrated wealth on elected officials may undermine the link between those officials and the public.[210] Yet, because campaign finance restrictions burden speech and associational rights, the Court has applied strict scrutiny—or, in some cases, exacting scrutiny—and in recent years it has increasingly invalidated such laws.[211]

In this section, I argue that content-based laws restricting the use of biometric targeting for political advertising would be analogous to campaign finance laws. Both would burden political speech (albeit only slightly) but would also serve compelling First Amendment interests related to preserving self-government. As with the Court's modern campaign finance jurisprudence, I warn that the Court would likely fail to

[209] *See, e.g.*, ALEXANDER MEIKLEJOHN, FREE SPEECH AND ITS RELATION TO SELF-GOVERNMENT 18–27 (1948) (explaining the First Amendment "paradox" that some speech must be restricted in a "well-governed society" and using the old town hall as a metaphor to demonstrate this point).

[210] *See* Scott Bloomberg, *Democracy, Deference, and Compromise: Understanding and Reforming Campaign Finance Jurisprudence*, 53 LOY. L.A. L. REV. 895, 920–26 (2020) (describing the treatment of the government's interest, in campaign finance cases, of ensuring legislative responsiveness to public opinion); Citizens United v. FEC, 558 U.S. 310, 446 (2010) (Stevens, J., concurring in part and dissenting in part); FEC v. Wisc. Right to Life, 551 U.S. 449, 507–22 (2007) (Souter, J., dissenting) (surveying both the history of legislative and judicial responses to the influence of "concentrated wealth" in elections, and both highlighting concerns with how such wealth degrades legislative responsiveness); s*ee also* ROBERT C. POST, CITIZENS DIVIDED: CAMPAIGN FINANCE REFORM AND THE CONSTITUTION 16 (Harvard Univ. Press 2014) (introducing the concept of "representative integrity" to describe the need for legislative responsiveness in a democracy).

[211] *See* McCutcheon v. FEC, 572 U.S. 185, 196–97 (2014) (plurality opinion); *Citizens United*, 558 U.S. at 365–66; *see generally* FEC v. Cruz, 142 S. Ct. 1638 (2022).

appreciate the nature and importance of the government interest(s) backing such a law, as well as the only modest burden on speech caused by the law. The Court would likely apply strict scrutiny and would almost certainly hold that a content-based restriction on the use of biometric targeting in political advertising fails that test.

First, I worry that the Court would fail to credit the broad privacy- and democracy-related government interests, described *supra* in Part II(B), that government would be pursuing by restricting biometric targeting in political advertising, leaving only an under-inclusive interest in protecting individual informational privacy and an over-inclusive interest in preventing foreign interference. That is because in the campaign finance context, the Court has rejected similar government interests pertaining to protecting democratic functions.

Indeed, in the campaign finance context, the Court's recent decisions have been marred by an extraordinarily narrow understanding of the interest pursued by governments when they restrict election spending. The Court has described the government interest as being limited to preventing the appearance or reality of "quid pro quo" corruption.[212] The government has a compelling interest in preventing the direct exchange of cash-for-votes, but beyond preventing such exchanges, the government cannot restrict the flow of money in elections.[213] Thus, the Court has held that restrictions on independent expenditures are categorically unconstitutional because *independent* expenditures carry no risk of a quid pro quo exchange.[214] The Court has also employed this narrow understanding of the government's anticorruption interest to invalidate aggregate contribution limits.[215]

Early campaign finance majority opinions, more recent dissenting opinions, and several prominent scholars have harshly criticized this "crabbed" view of the government's anticorruption interest.[216] These jurists and scholars advance a much broader

[212] *Citizens United*, 558 U.S. at 357–58 (framing the government interest in campaign finance cases in terms of narrow *quid pro quo* corruption); *see also* Bloomberg, *supra* note 210, at 914–19 (unpacking the narrow understanding of corruption advanced by some justices in campaign finance cases and contrasting it with a broader understanding advanced by others).

[213] *Citizens United*, 558 U.S. at 357–58.

[214] *Id.* at 365 (overruling Austin v. Mich. State Chamber of Com., 494 U.S. 652 (1990) and McConnell v. FEC, 540 U.S. 93 (2003)).

[215] *McCutcheon*, 572 U.S. at 208–09.

[216] *See, e.g.*, *McConnell*, 540 U.S. at 152 (opinion of Stevens, J.) (criticizing the dissent's "crabbed" view of corruption); *Citizens United*, 558 U.S. at 447 (Stevens, J.

conception of the government's interest in campaign finance cases: preserving "political equality" or "electoral integrity," or preventing amassed wealth from distorting the political process.[217] Under these broader conceptions of the government's interest, governments can restrict money in elections to protect, well, democracy. That is, governments can act to ensure that elected officials are responsive to the public rather than to the wealthy subset of the public that is able to spend virtually without limit in elections.

The jurists who subscribe to the crabbed view of corruption in campaign finance cases will likely advance a crabbed view of the government's interest in response to a content-based restriction on biometric targeting. Namely, proponents of ad-targeting will likely frame the government interest as an interest in protecting individual users' informational privacy—i.e., each users' ability to prevent their information from being shared or used in a manner that the user would not reasonably expect. Indeed, the Court has already taken a similar tack and adopted an unduly narrow conception of privacy harm in the Article III standing context.[218]

A repeat performance in the instant context would make it nearly impossible for limits on biometric targeting in political advertising to pass constitutional muster. If a reviewing court evaluates the law under an individual informational privacy framework—eschewing the broader privacy- and democracy-related interests described *supra*—the law could not survive strict scrutiny. A narrow interest in informational privacy may explain why biometric targeting should be prohibited across the board—on a content-neutral basis—but it would not explain why the government can single out the use of biometric targeting in political advertising. To justify that content-based restriction, the court would need to appreciate and credit the unique harms wrought by the ad-targeting practice in the political advertising

dissenting) (same argument as in *McConnell*, but in dissent); LAWRENCE LESSIG, REPUBLIC, LOST: HOW MONEY CORRUPTS CONGRESS – AND A PLAN TO STOP IT 241–43 (2011) (critiquing the *Citizens United* Court for conceiving of corruption only in terms of quid pro quo exchanges and failing to recognize the type of corruption caused by legislative dependence on wealthy campaign financiers).

[217] POST, *supra* note 210, at 61–62; *Austin*, 494 U.S. at 659–60; *see* RICHARD L. HASEN, PLUTOCRATS UNITED: CAMPAIGN MONEY, THE SUPREME COURT, AND THE DISTORTION OF AMERICAN ELECTIONS 186–87 (2016).

[218] TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2214 (2021); Daniel J. Solove & Danielle Keats Citron, *Standing and Privacy Harms: A Critique of TransUnion v. Ramirez*, 10 B.U. L. REV. ONLINE 62, 68–69 (2021) (criticizing the *Ramirez* Court for having an inadequate understanding of privacy harms).

context. Otherwise, the law would be grossly under-inclusive to a general informational privacy interest.

Whereas an individual informational privacy interest would render a restriction on biometric targeting for political ads under-inclusive, another interest the courts have credited in the campaign finance context would make such a law over-inclusive: preventing foreign interference in elections.[219] That interest is undoubtedly a compelling one, but the government does not need to restrict *everyone's* speech in order to achieve their goal of preventing the problematic speech. It could achieve the same objective by banning the foreign-funded biometric targeting of political ads.[220]

There is a second issue involving the Court's understanding of the government interest in campaign finance cases that will prove instructive in the instant context as well. In campaign finance cases, liberal Justices have taken the position that First Amendment interests "lie on both sides of the legal equation."[221] These Justices mean that when the government restricts spending in elections, the restriction not only *harms* First Amendment interests by restricting speech, it also *furthers* First Amendment interests by creating a marketplace for speech in which the public's views can be heard and responded to by elected officials.[222] Given that such speech restrictions further First Amendment objectives, these Justices find strict scrutiny inappropriate. Instead, they would apply a less skeptical form of judicial review, giving governments more leeway to manage the democratic process.[223]

The same reasoning applies to restrictions on the use of biometric targeting in political advertising. Even if such

[219] *See, e.g.*, Bluman v. FEC, 800 F. Supp. 2d 281, 288 (D.D.C. 2011) (opinion by Kavanaugh, J.), *sum. aff'd* 565 U.S. 1104 (2012) ("[T]he United States has a compelling interest for purposes of First Amendment analysis in limiting the participation of foreign citizens in activities of American democratic self-government, and in thereby preventing foreign influence over the U.S. political process.").

[220] *See* John M. King, Note, *Microtargeted Political Ads: An Intractable Problem*, 102 B.U. L. REV. 1129, 1148–49, 1159 (2022) (highlighting the same over-inclusiveness problem in the online political ad microtargeting context); Wash. Post v. McManus, 944 F.3d 506, 520–22 (4th Cir. 2019) (crediting the government's interest in preventing foreign election interference but concluding that the interest did not justify imposing certain transparency requirements on publishers of political advertisements).

[221] *McCutcheon*, 572 U.S. at 235 (Breyer, J., dissenting).

[222] *See* Bloomberg, *supra* note 210, at 928 (identifying this position).

[223] *Id.* (discussing Justice Breyer's position in Nixon v. Shrink Missouri Gov't. PAC, 528 U.S. 377, 402–03 (2000) (that the Court should take a more deferential posture in campaign finance cases).

restrictions would (in some sense) restrict speech, they would also further Speech Clause objectives that are important to sustaining self-government—preventing filter bubbles and protecting intellectual privacy.[224] This undermines the case for applying strict scrutiny in the first place and suggests that such restrictions, like most campaign finance restrictions, should be evaluated under a less hostile standard of review.

Third, in the campaign finance context, the Justices have disagreed about whether restrictions on corporate election spending constitute bans on corporate speech, or instead merely change the means through which corporations must speak. Prior to *Citizens United*, federal law prohibited corporations from making independent expenditures funded by their general treasury accounts but allowed corporations to establish separate segregated funds ("SSFs")—funded by relatively small contributions by employees, shareholders, and members—from which they could make expenditures.[225] To the *Citizens United* majority, this restriction constituted an "outright ban" on corporate-funded speech, amounting to censorship, notwithstanding the availability of speaking through an SSF.[226] To the *Citizens United* dissenters, the burden on speech imposed by federal law fell far short of an "outright ban;" rather, the law merely regulated the channel through which corporations had to speak (through an SSF, rather than a general treasury account).[227]

I anticipate a similar disagreement in the present context. Libertarian jurists are likely to view a restriction on biometric targeting as a significant restriction on speech; one that bans a valuable tool that speakers can use to reach their desired audience. However, the speech burden imposed by a prohibition on the biometric targeting of political ads is far more modest—it does not limit what speakers can say, how much they can say it, or even to whom they can say it. Instead, it imposes a relatively minor efficiency burden on speech. Speakers cannot target their messaging quite as efficiently as they otherwise would, but they would still be able to spread the same message to the same or similar listeners by using somewhat less exacting targeting tools. The primary difference is that more people will hear the message

[224] *See supra* Part II(B) (discussing the significance of preventing filter bubbles and preserving intellectual privacy to First Amendment jurisprudence).
[225] *Citizens United*, 558 U.S. at 321 (explaining the SSF system).
[226] *Id.* at 337.
[227] *Id.* at 419 (Stevens, J., concurring).

(because it will not be so acutely targeted), and, because more people will hear the message, it will cost the speaker some marginal amount more to reach the segment of the audience they would have reached by employing biometric targeting.

The marginal decrease in the efficiency of speech caused by a restriction on the use of biometric targeting would indeed burden speech, thus making some First Amendment analysis appropriate. But it would be a far cry from the exaggerated claims of censorship used to justify the application of strict scrutiny and the subsequent invalidation of laws in campaign finance cases.

***

This First Amendment analysis reveals a field of landmines for policymakers trying to restrict the use of biometric targeting in political advertising. Content-neutral restrictions will likely face political barriers. Even if enacted, opponents will leverage the Court's speech clause jurisprudence to frame seemingly content-neutral laws as actually being content-based. And even if they fail at that threshold step, the opponents would still have several avenues to victory in an as-applied, political speech challenge to a content neutral restriction on biometric targeting.

Content-based restrictions will prove even more fraught under the Court's current First Amendment jurisprudence. If the Court's analogous campaign-finance cases are any indication, such restrictions will be subjected to strict scrutiny, the government interests involved will be minimized, the modest speech restrictions will be characterized as oppressive censorship, and the law will be struck down.

V. CONCLUSION & CONSEQUENCES

The promises of VR technologies sound a lot like the promises of the internet at its dawn: It will greatly increase our interpersonal connectivity and unleash a wave of creative expression, all while generating new economic opportunities for the public. As with the internet, we must strive to achieve those promises while mitigating the potential for harm posed by the new technology. That task will leave privacy scholars with much to write about over the coming years: VR technologies enable the collection and deployment of personal data at a virtually unimaginable scale.

This Article identified a particularly alarming problem with VR technology: Data collected using biometric monitoring can be used for political ads; that practice will exacerbate existing problems with political ad microtargeting; and the Supreme Court's current First Amendment jurisprudence will make it difficult for U.S. governments to constitutionally address those problems. As with other problems with VR, this will be one that scholars and jurists will continue to grapple with as the technology advances and gains more widespread adoption.

While the primary purpose of this Article is indeed to identify this emerging First Amendment problem, let me close by highlighting two consequences that flow from the Article's analysis.

First, the First Amendment uncertainty makes private ordering solutions all the more important. Public interest organizations are already working to ensure that companies design VR environments with privacy and safety in mind. For example, the XR Guild is a newly formed association of developers, researchers, lawyers, business executives, and other professionals who are working to establish a commonly-held set of ethical principles to guide the development of XR technologies.[228] The XR Safety Initiative is a similar group that is working to create standards for privacy, safety, security, and ethics in VR environments.[229]

These organizations and others should work to establish industry-wide rules governing the use of XR technologies in political advertising. Those rules should include restrictions on biometric targeting and other advanced targeting techniques, as well as the use of deepfake technologies. Transparency rules—while not sufficient to prevent the harms discussed in this Article—will also be important to establish if governments fail to act.[230] Providing users with information about whether political messaging is sponsored, who has paid for it, how it is

[228] Rosenberg, *supra* note 4, at 2 (explaining that the term "XR" is "commonly used as a catch-all for all forms of immersive media," encompassing both virtual reality and augmented reality); *see* XR GUILD, http://www.xrguild.org (last visited Aug. 3, 2022).

[229] XR SAFETY INITIATIVE, *Who We Are*, http://www.xrsi.org/who-we-are (last visited Aug. 11, 2022).

[230] *See generally* The Honest Ads Act, S.1356, 116th Cong. (2019-2020) (imposing some much-needed transparency requirements on online political advertisements).

targeted, and whether it involves deepfake technology can help users evaluate the merits of campaigns' messages.[231]

Establishing these rules on an industry-wide basis will be particularly important. As it stands, each major online platform has their own rules for political advertising. The rules are wildly inconsistent, ranging from complete prohibitions, to limits on targeting, to mere transparency rules.[232] Platforms also use varying definitions to determine what constitutes a political advertisement that is subject to their self-imposed regulations.[233] This patchwork of self-governing policies should not carry over to VR environments. No company should gain a competitive advantage by maintaining lax rules around political advertising, and users should have the same protections no matter which platform's VR environment they access.

Private-sector solutions carry understandable skepticism; a skepticism that I share. Companies act in the best interest of their shareholders and that does not always align with the interests of users or society writ-large.[234] Accordingly, the costs of failing to adopt industry-wide standards for political advertising (and other ethical rules for VR technologies) must exceed the benefits. If a platform refuses to sign on to an industry-wide rule, users must boycott, employees must protest, journalists must shine a light, and commercial advertisers must threaten to take their business elsewhere. We must exact a financial toll if companies allow targeted political advertising in VR environments to go unchecked.

[231] *Cf.* King, *supra* note 220, at 1154–55 (proposing transparency measures in light of the First Amendment problems with restriction political ad microtargeting).

[232] *Compare* GOOGLE, *Advertising Policies Help: Political content*, https://support.google.com/adspolicy/answer/6014595#zippy= (last visited Aug. 9, 2022) (restricting targeting practices), *with* META, *Ads About Social Issues, Elections or Politics*, https://www.facebook.com/policies_center/ads/restricted_content/political (last visited Aug. 9, 2022) (not restricting targeting practices), *and* TWITTER, *Business: Political content*, https://business.twitter.com/en/help/ads-policies/ads-content-policies/political-content.html (last visited Aug. 9, 2022) (prohibiting political ads), *and* TIKTOK, *TikTok Advertising Political – Industry Entry*, https://ads.tiktok.com/help/article?aid=9550 (last visited Aug. 16, 2022) (prohibiting political ads).

[233] *See id.*

[234] *See, e.g.*, Christiano Lima, *Facebook knew ads, microtargeting could be exploited by politicians. It accepted the risk.*, WASH. POST (Oct. 26, 2021), https://www.washingtonpost.com/politics/2021/10/26/facebook-knew-ads-microtargeting-could-be-exploited-by-politicians-it-accepted-risk/ (reporting on the Facebook Papers leak, showing that the company knew its targeting tools would be used to spread misinformation).

Second, this Article's analysis provides further evidence that the current libertarian First Amendment jurisprudence is unsustainable. As data surveillance becomes more intrusive, extending even to our involuntary biological reactions, it will become increasingly indefensible to assert that the freedom of speech almost always prevents government from restricting data flows to protect privacy (and democracy). Rather, courts should adopt a First Amendment framework—like, for example, the attentional-choice model championed by Professor G. Michael Parsons—that would give governments more leeway to impose sensible restrictions on political ad microtargeting.[235]

[235] *See* Parsons, *supra* note 69 (criticizing the Court's understanding of the marketplace of ideas and arguing that, under an attentional-choice speech framework, microtargeted advertising constitutes anticompetitive conduct in the marketplace for ideas).