

Shockvertising, Malware, and a Lack of Accountability: Exploring Consumer Risks of Virtual Reality Advertisements and Marketing Experiences

Abraham Mhaidli, *University of Michigan, Michigan, 48109, USA*

Shwetha Rajaram, *University of Michigan, Michigan, 48109, USA*

Selin Fidan, *University of Michigan, Michigan, 48109, USA*

Gina Herakovic, *University of Michigan, Michigan, 48109, USA*

Florian Schaub, *University of Michigan, Michigan, 48109, USA*

Abstract—Companies are increasingly using virtual reality for advertising. This begs the question: what risks does VR advertising pose for consumers? We explore this question by analyzing VR marketing experiences (VRMEs) to identify risks and discuss opportunities for researchers, industry, and legislators to address these and future risks in VR advertising.

Virtual Reality (VR) marketing, i.e., marketing that utilizes the VR medium to promote or advertise a product, is becoming increasingly popular. Marketers highlight how VR can offer many benefits, such as increased immersion, interactivity of the medium, and the ability to digitally recreate products with relative high fidelity. With these benefits, VR allows for new and exciting ways to market products to consumers.¹

However, the increasing use of VR for advertising and marketing raises questions on what potential risks and harms VR advertising poses to consumers.² For instance, scholars have voiced concerns about privacy risks associated with VR advertisements (given the vast data collection capabilities of VR headsets)^{3,4} and the potential for manipulation and deception.² The history of advertising surely warrants a critical assessment of advertising in VR. Malicious mobile advertisements can redirect users towards malware.⁵ Ads can cause distress, particularly if they include graphic content.⁶ This raises questions over how these harms may translate to VR and what new harms may emerge, given that VR advertising can be more immersive and interactive than non-VR advertising.²

In this article, we approach this issue in two parts. First, we report on an analysis of current VR marketing experiences (VRMEs)—a prominent way in which companies leverage VR to engage potential customers. We identify multiple risks associated with VRMEs: we observe the use of shockvertising (advertisements which can cause shock and distress in users), the use of proxemic interactions to open links without user knowledge or consent, and a lack of transparency over data practices. Second, we extrapolate from these findings to discuss how the identified risks could evolve into significant harms in a world where VR advertising becomes mainstream.

Combined, we present a view into some of the risks and harms of VR advertising and marketing. Understanding these risks and harms is a critical first step for mitigating and addressing them. As VR technologies develop, VR advertising is likely to proliferate, and so are potentially harmful advertising practices. We conclude by discussing opportunities for researchers, industry, and regulators to address risks associated with VR advertising.

EXAMINING VRMEs

Our first step in this work is analyzing existing VR advertisements to surface potential consumer risks. One thing to note is that the number of advertise-

ments in VR is quite limited today, at least in terms of how we commonly understand advertisements (e.g., unskippable short videos or banner ads). However, a quite concrete instantiation of advertising in VR is the VR Marketing Experience (VRME). We use “VRME” to describe a VR experience whose primary purpose is the promotion of a brand, product, or service. They are often standalone experiences, relatively short in terms of duration, and free of charge. One example of a VRME is IKEA’s VR Experience (see Figure 1). It is a short experience which introduces users to IKEA furniture, allowing them to walk around a virtual house and explore furniture options. Another VRME is Expedia Cenote VR (also Figure 1). This VR experience, made by Expedia (a travel company), introduces users to the Cenotes, which are natural cave formations formed in the Yucatan Peninsula. It lets users walk around a virtual Cenote and displays facts about the Cenotes. At the end of the experience, users are encouraged to book a trip to see Cenotes in real life.

We focused our analysis on VRMEs as they can highlight trends in how VR advertising is developing and what are potential risks VR advertising could pose.

Analysis Approach

We followed a systematic process to identify current VRMEs. Since there were no keywords we could use to reliably filter for VRMEs, we manually reviewed all listings in three popular storefronts for VR applications (the Steam store, the Oculus Quest store, and the Oculus Rift Store). To develop a shared understanding of the VRME definition, the authors independently labeled a subset of VR experiences as either VRMEs or not VRMEs and aligned the ratings as a group, until a high inter-rater reliability was reached. Then, the authors subdivided the remainder of VR application search results to categorize independently, flagging ambiguous examples to discuss later on as a group and reach a consensus. To identify VRMEs, the authors analyzed each app’s description, metadata (e.g., price, genre, developer), trailer videos, and images, seeing whether the experience matched our VRME definition. Items we considered were: does the experience’s store description explicitly mention that it was a branded experience? Were there references to real-world brands and services present either in the description or in the store page? Did users post comments on the VR store page mentioning that this was an advertisement/marketing? In total, we reviewed 8,227 VR application listings and identified 87 standalone VRMEs.

We then used a qualitative walkthrough approach⁷ to study the VRMEs, with at least two authors an-

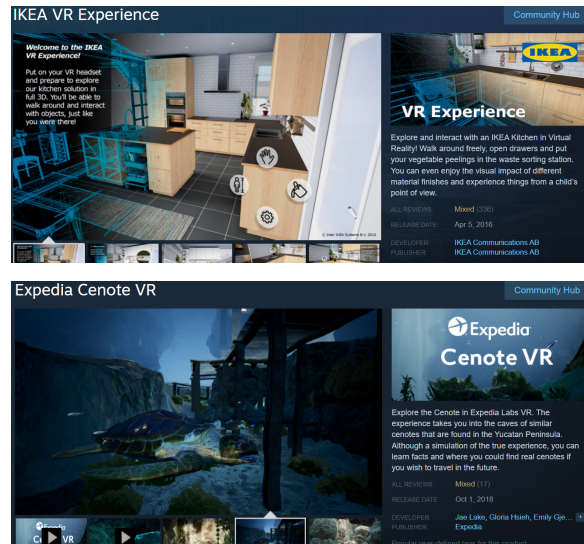


FIGURE 1. Two VRME examples. From top to bottom: (1) A screenshot showing *IKEA VR Experience* experience on Steam. It is a short experience which introduces users to IKEA furniture, allowing users to walk around a virtual house, explore furniture options and learn about them. (2) A screenshot showing *Expedia Cenote VR* experience on Steam. This VR experience, made by Expedia (a travel company), introduces users to the Cenotes, which are natural cave formations formed in the Yucatan Peninsula. It lets users walk around a virtual Cenote and displays facts about the Cenotes. At the end of the experience, users are encouraged to travel there in real life. For both experiences, the store description is shown on the right.

alyzing each experience together. One author was assigned to play the VRME from start to finish, so as to encounter all of its immersive content and interactions. The other author(s) watched the live-streamed first-person view of the experience on a monitor and took notes on the VRME, documenting the experience and potential risks encountered. We also recorded the first-person video of each session. To ensure that we discovered as many scene elements as possible, we watched the trailer videos and read other users’ comments on the app store pages to surface any additional interactions we may have missed in our play sessions. After playing through the experience, members of the research team collectively discussed the experience, then revised and updated the notes as needed.

One area of concern with VR advertising are associated privacy risks.^{3,4} Through various sensors (including cameras and microphones), VR headsets can track a user’s body movement, gaze direction, heart rate, pupil dilation, facial expressions, as well

as information about their surrounding environment⁸ — information which could be used to infer individual user characteristics for ad targeting and personalization. Thus, we also documented whether a VRME had a privacy policy, or another document that described its data collection practices (e.g., EULA or ToS). We then analyzed these policies to understand the VRME's data collection and use practices.

Corpus Characterization

The 87 analyzed VRMEs promoted a wide range of products, including movies and TV shows (21), technology (14), tourism (12), food and beverage (8), housing and design (7), careers (6), video games (6), automotive (5), education (3), sports (2), paint (1), chainsaws (1), and hot tubs (1). Similarly, we saw a wide number of publishers and developers behind the VRMEs: for the 87 VRMEs, there were 81 different developers and 82 different publishers, showing that the field is dynamic with many different companies making VRMEs. Most VRMEs were short with a median play time of 13:05 minutes (mean 14:53 minutes), ranging from 2:18 to 45:00 minutes.

Finally, we used the number of reviews as a proxy for how popular the VRMEs were. VRMEs mostly had few reviews, with a median of 23 reviews across both stores. However, a few VRMEs were very popular, with reviews in the hundreds or even thousands. These were mostly VRMEs related to promoting movies, such as *Jurassic World: Apatosaurus* (23,311 reviews), *Spider-Man: Far From Home Virtual Reality* (1,767), or *Coco VR* (924).

KEY RISKS IDENTIFIED IN VRMEs

We identified five key risks in current VRMEs: the use of shockvertising in VR; having users carry out controversial tasks; a lack of exit options; using proxemic interactions to open web links; and a lack of transparency over data practices.

Shockadvertising

We found that several (16) VRMEs subjected users to potentially distressing experiences. These included: being chased by a giant, falling from a building, passing out due to dehydration, being knocked out in a boxing match, being eaten alive by a snake, watching a coworker die, having to escape a military compound, getting beaten up, being tortured, being trapped in a zombie warehouse, navigating through spinning blades of death, and being hunted by aliens. Additionally, we identified ten experiences where the user either could

die or would die as part of the experience. The purpose and context of these distressing events differed. For some VRMEs, the distressing event was closely tied to the product being advertised; for example, the VRME *Belko VR: An Escape Room Experiment* promoted a horror movie, and so the experience 'previewed' the horror movie. In other experiences, the distressing event served to highlight the importance of a product; for example, the *Beat The Blitz* VRME had the user pass out due to dehydration as a way to educate the user on the importance of staying hydrated. See Figure 2.

This phenomenon of 'shockvertising' (the use of shocking and distressing content to promote a product) is not new to advertising.⁶ However, the key difference is that in VR, one is not just passively observing shocking content on a screen; in VR, the shocking and distressing content is directly happening to the user. The risks of shockvertising may be subtle at first. VRMEs are opt-in, meaning that users might choose to experience distressing events. However, the issue arises when users are not aware or informed about a VR experience containing such distressing events. Many VRMEs did not warn of the exact nature of the distressing event on the store page. Moreover, it is possible that VR advertising advances to a point where VR ads are not standalone but rather integrated into other primary VR experiences, meaning that users are experiencing distressing events they did not opt-into.

Enacting Controversial Tasks

Relatedly, a few VRMEs (5) had users perform tasks or activities that could be perceived as controversial or morally objectionable. Specifically, some VRMEs had the user smoke drugs out of a bong, jump off a building, commit suicide by shooting themselves in the head, and make potentially traumatic decisions (e.g., whether to save a coworkers life or one's own, or whether to execute a prisoner). Most of these activities were optional, but some were required to play through and complete the VRME.

The use of controversial tasks could fall under the banner of shockvertising, since the effect is the same: using shocking or distressing content to promote a product. However, one key difference from traditional shockvertising is that rather than watching a shocking or disturbing event, in VR the users *themselves* perform the controversial and potentially distressing task. There is work that suggests that performing an action in VR is recorded by the brain in ways similar to performing the action in real life.¹⁵ Depending on the scope of the action, this could open up ways to hurt

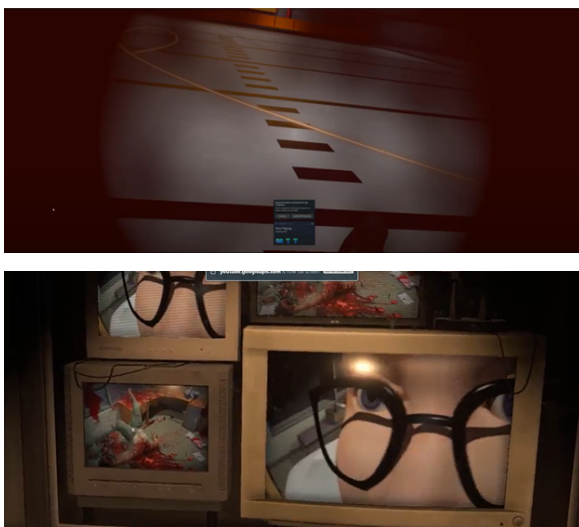


FIGURE 2. Two distressing events in VRMEs. From top to bottom: (1) A screenshot of *Beat The Blitz*, a VRME promoting a sports drink. In the screenshot, the user is passing out due to dehydration. The vision is narrowing and slowly turning red. During the experience, loud palpitations were heard. (2) A screenshot of *Belko VR: An Escape Room Experiment*. The user is watching a corpse through a TV screen, and must decide whether to kill a co-worker to save themselves.

or harm users if the action to be taken is particularly traumatic, or if a user is particularly opposed to that action.

Lack of exit options

In many VRMEs (51), once the user started the experience, it was very difficult to pause or exit. To quit the VRME, one had to either fully exit the experience using the built-in Oculus or Vive menus (i.e., a lengthy press of the Oculus/Vive button) or physically remove the headset.

Our findings show that not being able to easily exit or skip a VRME poses potential health and safety risks. We identified multiple VRMEs with distressing content that could cause emotional harm to users. There may be VRMEs with other harms, such as those that contain flashing images, excessively loud noises, or badly-optimized experiences that induce motion sickness in the user. This lack of appropriate exit options, such as being able to skip or exit problematic ads, thus perpetuates these more substantial harms.

Proxemic interactions open links without user awareness

Two experiences (*Expedia Space Needle VR* and *Expedia Cenote VR*) used the user's location in VR, e.g., standing in a certain spot, to open a link in the user's web browser. There was no indication within the VR app that standing in that spot would open a website, or that one had been opened—it was only visible once the user exited the app that the website had been opened.

While in this instance the links that were opened were benign, one can imagine that the same technique could be used to open more nefarious links (e.g., malware).

Lack of transparency over data practices

Overall, there was a concerning lack of transparency over the data practices of VRMEs, given privacy concerns with the expanded sensing and data collection capabilities of VR headsets. Only 26 of the 87 VRMEs we analyzed provided working links to a privacy policy; a further 12 VRMEs provided a link to either an End User License Agreement (EULA) or a Terms of Service (ToS), but not a privacy policy. The presence of these links was highly correlated with the store the experience was found in: all VRMEs in the Oculus stores provided a privacy policy and/or Terms of use, as Oculus requires a privacy policy link as part of the publishing process. In contrast, only 17 out of 73 VRMEs on the Steam store provided a privacy policy or an EULA. In fact, 13 experiences that were present in both Steam and Oculus stores provided a privacy policy in the Oculus store, but not in the Steam store.

Out of the VRMEs that had privacy policies, EULA, or ToS documents, 23 mentioned using collected user data to either personalize or target advertisements and marketing materials. However, none of them specified how or to what level that personalization occurred, raising questions as to how privacy invasive this personalization is.

One interesting note is that 24 VRMEs linked to their publisher's general privacy policy or terms that only talked about data practices in broad and abstract terms with no information about the specific data practices of the analyzed VRME. By contrast, only 14 were specific to the experience.

ANTICIPATING EVOLVING HARMS

Our analysis uncovered multiple potential risks VRMEs can pose to users. While VRMEs, and advertising in VR more generally, are not yet mainstream and current VRMEs are typically standalone experiences

(i.e., users have to choose to engage with them), our findings provide indications for how VR advertising might evolve in the future, and how the risks of VRMEs (if left unchecked) may evolve with them. In this section, we extrapolate from the identified risks to how risks and harms may manifest in future forms of VR advertising.

To do so, we first need to *imagine how the VR advertising ecosystem will develop*. First, let us assume a world where VR headsets are more widely used than they are now; perhaps they are not quite as ubiquitous as smartphones or laptops are today, but they are widely used enough to warrant interest from advertisers to put advertisements in VR. In this world, we can imagine that there will be *more refined advertising approaches and types*. Rather than standalone VR experiences a user needs to opt into, we can imagine advertisements more closely embedded in content a user would usually enjoy, such as in-app advertisements for popular VR apps. Additionally, there may be more subtle forms of advertising such as product placement. As such, we can imagine that a majority of advertisements will not be opt-in, but rather, be foisted upon the user. The user may know they will encounter an advertisement, but unlike with current VRMEs, they will not know which specific advertisement they will run into, or exactly when they will see it.

Alongside more refined ad types, the process for how these ads appear will become more widespread. Currently, VRMEs are made by individual companies who develop and post their VRME on an app store for users to find. In a world where there are more VR advertisers and a more mature VR advertising ecosystem, the process by which VR users see advertisements may be more complicated and mediated by advertising networks or through bidding processes (similar to how social media and mobile app advertisements are handled today). Rather than each advertisement being vetted and approved, there is a bidding process via which various companies pay to advertise to users based on their demographics, and behind-the-scenes algorithms decide who to show an ad to based on the amount bid by the company and perceived fit. This could be coupled with extensive forms of data collection to microtarget ads towards individual users—for example, VR experiences could embed subtle tasks in their interactions to assess a user's personality traits, then use that information to live target advertising, and show the user the ad from the highest bidder.

Lastly, we can also expect an increased level of sophistication in VR development, to the point of having photorealistic graphics, more advanced and detailed sensors able to capture all types of user data, and

even being able to emulate senses beyond sight and hearing, such as touch, taste, or smell, as well as more interactive forms of advertising and marketing experiences, which the highly interactive VRMEs we analyzed point towards.

With these factors in mind, we next extrapolate how the risks we found in VRMEs may morph into more substantial harms. A summary of these harms can be found in Figure 3.

Unskippable, traumatic advertisements

Our findings regarding distressing experiences in VRMEs suggest a real risk that users could be forced to interact with VR ads that have distressing moments. Perhaps in the future there is a VR ad for an upcoming horror movie that has users being chased by a machete-wielding serial killer and be brutally murdered. Whereas current VRMEs are opt-in, in an increasingly sophisticated VR advertising environment, we can imagine that a user being put through this ad is not aware of its content before engaging in it—maybe they were playing a game of a completely different genre and were not expecting a machete-infused VR ad horror show. Advanced graphics could make this experience particularly disturbing, coupled with immersive audio and possibly incorporating other senses (e.g., smell, touch) to increase realism. Alternatively, these traumatic advertisements could involve the user enacting or recreating a controversial task. An ad for a gun company may have users shoot at individuals with a gun, which the user may be opposed to. These types of unskippable, traumatic advertisements could be particularly problematic if the users seeing this advertisement are children. Although marketed for adults, VR headsets do have a substantial underage user base.⁹ This raises a potential danger of children being shown shockvertising content.

Perhaps most importantly is the fact that it will be very difficult, if not impossible, to skip or avoid the ad in VR. In non-VR advertising, one can look away, walk out of the room, put a device down, or otherwise easily ignore an advertisement. The immersive nature of VR headsets makes this task difficult for VR advertising. VR headsets, almost by definition, are designed to block out the real world and immerse users in a completely virtual world. This means that traditional evasion methods (e.g., looking away to ignore the ad) do not work the same way for VR advertising (see Figure 4). Presumably one could close their eyes to avoid seeing the ad, but this would not block out audio or other senses—furthermore, cameras in the VR headset could detect whether a user has closed their

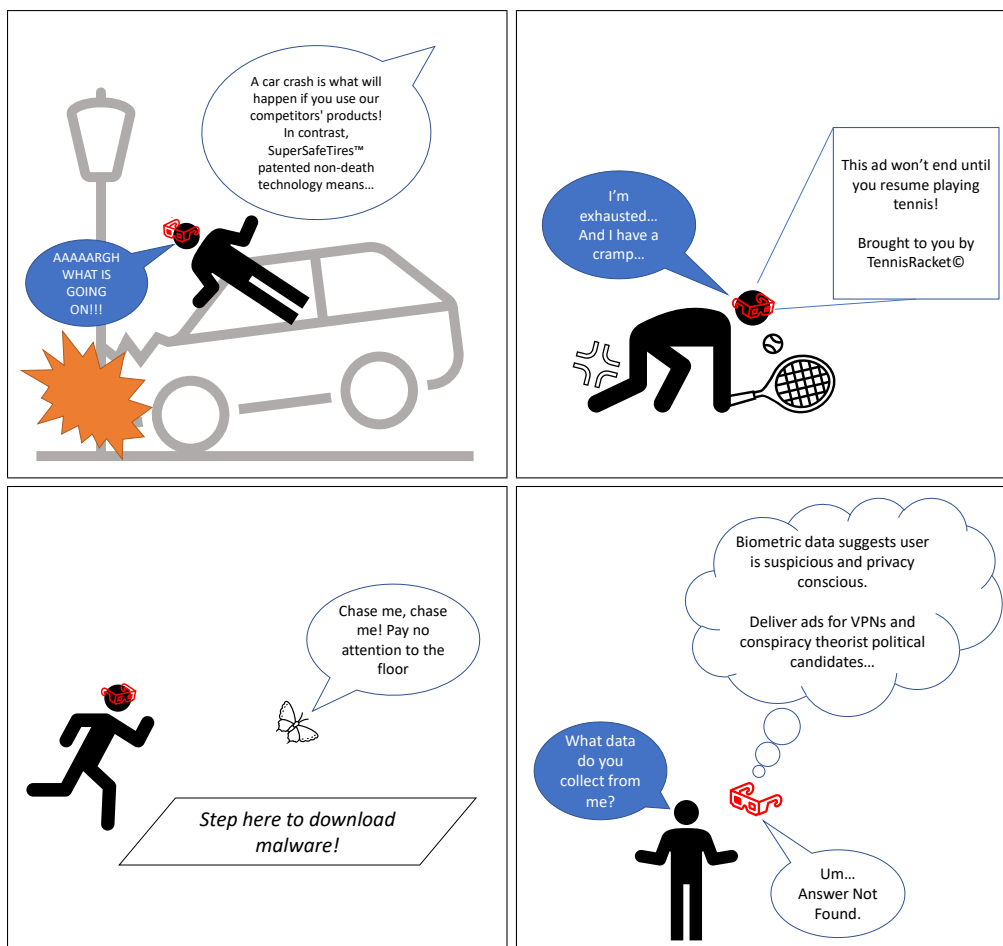


FIGURE 3. A summary of the evolving harms of VR advertising. *Top-left:* Shockvertising—VR ads may display distressing content to users. In this case, to make users fearful of competitors' products, a VR ad may have users experience dying in a car crash to highlight the safety features of their own product. *Top-right:* Interactive VR ads may require intense physical movements to complete and finish the advertising—physical movements that could injure a user or which the user is unable to carry out. *Bottom-left:* VR advertisements may use proxemic interactions to open weblinks. Malicious VR ads may distract users with content (e.g., chasing butterflies or some animated object) to make them unaware of their interactions with their environment. *Bottom-right:* VR ads can collect biometric data from users and use it to target advertising. Without clear requirements for disclosure, what information is being collected by VR advertisers and how that information is being used will be hidden from the user, who may object to their data being leveraged for advertising purposes.

eyes and not end the ad until the user reopens them. This could be solved through an exit option within the advertisement; however, we believe it is unlikely for these exit options to exist. First, from our analysis of VRMEs, we saw that many did not provide users with exit options, with the only option being completely removing the headset. Additionally, it is unlikely VR advertisers will have incentives for developing these exit options—why would companies spend large sums of money on an ad just to develop mechanisms for users to easily bypass and skip them? Completely

removing the headset has the problem of exiting an entire experience. This may work to exit standalone VRMEs, but in a future with in-app advertisements, consumers may be forced to miss out on good content and shut down entire applications, all to avoid one disturbing moment.

Physical Harms from VR Ads

Another unintended harm that arises from VR advertisements is that of physical harms. Some of the VRMEs we played through were gamified and interac-

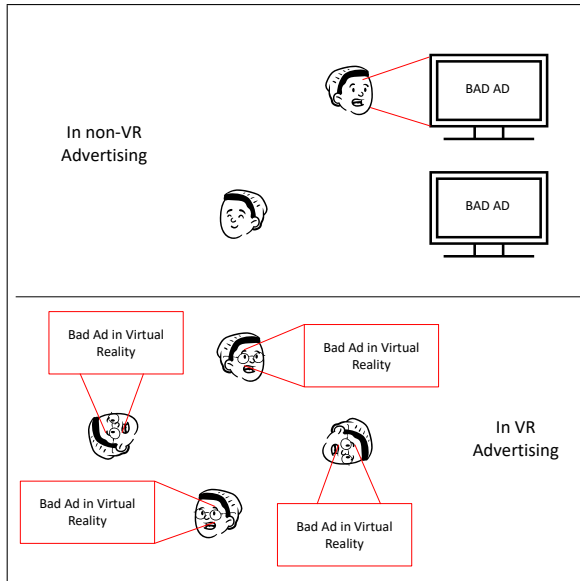


FIGURE 4. Why a lack of exit options in VR is problematic: in non-VR advertising (*top*), if encountering a bad or distressing advertisement, one can look or walk away. In VR (*bottom*), this becomes much more difficult, given the immersive nature of the VR headset, such as 360 field of view, meaning no matter where the user looks, they will see the problematic VR ad. Since ads are much more difficult to avoid and ignore in VR, the need for ways to quickly skip or bypass advertisements is crucial.

tive, sometimes requiring physical activity to complete the advertisement. Some of this physical activity could be quite strenuous; while playing through one of the VR ads, one of the authors got a muscle cramp. Interactivity in advertising is nothing new—there are non-VR ads which have some level of interactivity (e.g., some mobile app advertisements require users to complete a puzzle or finish a minigame to end the advertisement). However, the scope and scale of how the interactivity works are orders of magnitude larger in VR. Rather than swiping a cursor using a mouse, or tapping on a few buttons on a phone screen, VR can have you perform a wide array of movements, including complex hand gestures, moving from one location to another, jumping, dancing, ducking, crouching, and much more. Similarly, with VR, the interactivity can be forced or compelled from users much more effectively than in mobile apps. In an interactive mobile advertisement, if the user is not up to performing a task, the user can easily walk away, put the phone down, or otherwise disengage from the advertisement. In a VR ad, the user may not be afforded that privilege. The VR ad

can ‘come at you’ to get you to move, such as through digital avatars that come tackle you and which you must avoid.

As VR ads evolve, one can imagine a future where unskippable in-game VR ads require some type of physical movement by users. Maybe the movement is as simple as dragging one object from one location to another, or it may be more complex (the user must enact a series of dance moves in precise order to complete and bypass the ad). The physical requirements of the in-app ad may differ from the physical requirements of the VR experience, and the user may not be able to complete the physical demands of the ad. In these cases, the ad could represent possible accessibility issues or possibly even threats to physical safety in cases where the demands of the VR ad cause the user to crash into a wall or their furniture, with VR ads that are badly optimized, or with VR ads that have strobing and flashing lights which may trigger seizures.

New ways for introducing malware and spam

We observed two VRMEs that opened links without users’ knowledge or consent, triggering as the user walked into a specific area. In a future where VR advertising is more common, it is possible that bad actors will use these same techniques to have the user open weblinks without them noticing or realizing. The potential harm with having proxemic interaction invisibly trigger the opening of links is that users may open links they do not want to open, or open links they are not even aware of being opened. In these two VR ads, the links opened to a booking page for the relevant tourist destinations. However, the effects could be much more severe. The effects of this may range from annoying (opening a link that interrupts the experience) to possibly dangerous in the case of opening links to malware or phishing sites.

Furthermore, this interaction technique could be used for actions beyond opening malicious links. For example, a VR shopping app could measure when a user stands in a certain location, and use this to trigger a purchase. If there is no clear guidance that this can occur, users may unwittingly walk into these trigger locations. Even in cases where the link opened is not malicious, it can still be annoying. Marketers may leverage the annoyance these constant interruptions create to nudge the user into a certain action. For example, every step a user makes opens a link encouraging the user to sign up for a newsletter, and it is only once the user has signed up for the newsletter that the links stop popping up.

Lastly, as VR develops, there may be even subtler

ways users can inadvertently opening links, including certain hand gestures, voice commands, or other types of interactions.

Lack of accountability over data practices

The VRMEs we analyzed did not properly disclose their data practices through their privacy policies. Most did not have a privacy policy, and even if they did, it was difficult to ascertain what the data practices were. As VR headsets evolve, the type and quantity of data they will collect will evolve as well. By failing to properly disclose data practices, there may be a lack of accountability over how advertisers handle and leverage user data. Sensitive user data may be used to target user's vulnerabilities and manipulate them.^{2,3} Bad actors may use data to learn sensitive information about users and push for microtargeted advertising, such as political microtargeting.¹⁰

IMPLICATIONS FOR VR ADS

VR technologies, and VR advertising, are not yet mainstream. However, with recent announcements of upcoming headsets (Meta Quest 3, Apple's Vision Pro), it is reasonable to expect that these devices will eventually become mainstream—without action, the risks we identified in current VRMEs could morph into more serious and substantive harms. At the same time, we do not suggest or expect that all VR ads will display these risks or be shocking: in fact, it may only be a minority of ads that give cause for concern. However, the severity of potential risks, even if rare, makes it important to highlight and proactively address them. To that end, we conclude this article by discussing ways researchers, industry, and regulators can proactively address risks of VR advertising.

Guidelines for (Un)Acceptable VR Ads

One of the first orders of business is to further investigate (un)acceptable VR ad practices; in particular, given the possibility for distressing and controversial content in VR, there need to be rules determining what are acceptable distressing events allowed in VR. Is it ok to have VR advertisements where users are chased by serial killers and brutally murdered? Is it possible to create a taxonomy or list of controversial actions that an ad may force a user to do which should not be allowed (or at least, should be optional for users to complete an ad)?

More research is needed to understand what are acceptable and unacceptable VR ad types and tasks. This should be done in conjunction with key stakehold-

ers (e.g., VR users, VR marketers, VR app developers) to develop such guidelines. Similarly, the impacts of distressing and controversial VR advertising on users needs to be investigated. Can we demonstrate and/or quantify the harms that distressing advertising causes on users? Data demonstrating what the harms of these advertisements are would go a long way in convincing lawmakers and industry that this is a problem worth addressing and tackling.

From an industry and legislative perspective, guidelines for appropriate advertising content need to be adapted for VR. There are already guidelines governing certain aspects of advertising content—for example, the US Federal Trade Commission has guidelines on what is acceptable and unacceptable advertising towards children.¹¹ Existing guidelines need to be adapted to VR, where the nature of the virtual environment (more immersive and interactive, and an environment where a user actively participates in an ad instead of being a passive recipient) means that certain practices that are acceptable in non-VR mediums may become unacceptable in VR. For example, a mobile ad in which a car crash is shown may be acceptable, but a VR ad where the user *experiences* a car crash themselves might be a different matter.

Stringent Oversight Mechanisms

Even with these guidelines, VR platforms need to develop effective controls to limit the chances of bad advertisements appearing on VR platforms. One issue facing advertising on social media ecosystems is that social media companies often do not directly select the ads shown on their platform; instead, ads are selected through a bidding process whereby various advertisers pay to advertise on the platform. The large number of advertisers making bids likely means these companies do not vet every single advertisement. This means sometimes bad advertisers can 'slip the net' and show bad advertisements to consumers. In mobile apps, despite there supposedly being strict controls to prevent malware ads, there are countless ads bypassing these controls and exposing users to malware.¹² In VR, bad ads could be ones that show distressing shockvertising, ads that leverage proxemic interactions to show malware to users; or even ads that intentionally try to physically harm users (e.g., ads that deliberately have users bump into walls). The VR advertising ecosystem is fairly young; as such, it is the perfect time to create robust oversight mechanisms that go beyond current advertising models. This can include developing more stringent requirements for who is allowed to advertise in VR, or more oversight (e.g., creating advertising

models where VR companies vet and approve all ads before they can be shown on their platform, rather than a bidding process where there is little control over who is showing what type of ads).

Developing Adequate VR Exit Options

In addition to these guidelines, it is also imperative to develop exit options that allow users to quickly and easily exit VR. Quick exit options are more than simply a way to help consumers skip ads; it is primarily a safety feature to allow users to quickly bypass content that is distressing, disturbing, and in the case of badly optimized marketing materials, nauseating and possibly harmful. These could be voluntarily implemented by VR advertisers and/or VR platform providers, or mandated through regulation.

Currently, exiting apps is a feature provided by the VR platform. For example, Oculus and SteamVR both offer a 'quick menu' button to exit out of an experience. However, we argue that there needs to be additional mechanisms for shutting down problematic ads that do not come from the operating system. The main concern with operating-system level exit options is that they exit the entire experience. This may work to exit standalone VR ads, but in a future with in-app advertisements, consumers may be forced to miss out on good content and shut down entire applications, all to avoid one disturbing moment. Furthermore, in moments of panic or distress, users may not readily see or remember the quick exit menu button that is currently offered. Oftentimes in VR, controllers do not appear as controllers, rather they are represented as digital hands. For inexperienced users, or those undergoing a distressing ad, it might be difficult to remember to press a certain button on the controller or even find the button to press it while wearing the headset.

More research is needed to investigate what these exit options can and should be. Our findings suggest that, at a minimum, exit options should be easy to access, constantly present (meaning that the user does not have to remember complex buttons on the controller to activate), and allow the user to pause and exit the experience relatively hassle-free. But there are other considerations that need to be taken into account, since exiting VR suddenly can be disorienting.¹³

Standardize Privacy Policy Requirements

It was jarring to see that the same VRME could appear in one store with a privacy policy and in another storefront without one. This demonstrates the important role of the platform provider in setting reasonable

requirements for VR apps to ensure that platform users are provided with information about an app's data practices. Moreover, privacy policies should be specific to the VRME rather than a company's general privacy policy. This would allow users to better understand (1) what data is being collected about them specifically and (2) how their data is used within the context of a VRME or VR ad. Our analysis demonstrated that current VRMEs' privacy policies are useless for consumers in attempting to understand those two aspects.

There is a long and complicated debate to be had over what data VR advertisements can collect from users and what should they be allowed to use that information for. At the very least, there should be standardized requirements for letting users know what data is being collected by a VR advertiser and how it is being used in VR. This would not only benefit users, but also benefit regulators and those seeking to audit VR advertisements to understand their data practices.

Proxemic Interaction Should Not Open Links

While we only found two instances of VR ads using proxemic interactions to trigger the opening of a link, it is a dangerous enough technique to warrant special consideration. Inspired by link-blocking approaches in other contexts (e.g., pop-up blockers), we propose that opening any link outside of the VR experience through actions within the VR experience (e.g., clicking, in-app location) should display the link to the user and require explicit confirmation from the user before the link is opened, as well as giving the user the option to not open the link.

Labeling VR Ads and Marketing

Having studied VR advertisements extensively, we argue that there is a need to explicitly label VRMEs and VR ads as advertising. Labels should encapsulate not only standalone VR ads, but also more subtle forms of advertising (product placement, in-app advertising) that may develop in the future, as well disclose whether an ad contains shocking content or controversial tasks. There are already models for how this can work: for example, the Google Play mobile app store informs users whether a mobile app contains ads and/or in-app purchases. VR storefronts, such as the Oculus store and the Steam store, should similarly indicate when VR experiences contain in-app advertising, as well as which experiences are standalone advertisements, and which ones contain branded content.

This labelling is important for two reasons. First, it will help consumers recognize advertising experiences. From a deception perspective, if consumers

are aware that they are experiencing an ad, they are better equipped to make an informed decision about the ad's message, since consumers understand the context behind the promotion and can better recognize (and counteract) manipulative or deceptive messaging within them¹⁴. Mandating disclosures would allow consumers to make a fair evaluation of a VR ad's message and an informed choice on whether to purchase a product.

Secondly, from a regulatory and research perspective, labelling VR ads makes them also easier to monitor and study. A significant portion of time and energy in our study went towards searching for and identifying VR ads—having a label, tag, or filter through which one could easily obtain VR ads would make them easier to analyze both by researchers and regulators, e.g., finding and auditing VR ads for compliance with relevant regulation.

ACKNOWLEDGMENTS

The authors would like to thank Michael Nebeling, Yixin Zou, Julie Hui, Kat Roemmich, and Kaiwen Sun for their feedback on earlier versions of this work. This research has been partially supported by the National Science Foundation (#2105734).

REFERENCES

1. B. Shen, W. Tan, J. Guo, L. Zhao, and P. Qin. "How to Promote User Purchase in Metaverse? A Systematic Literature Review on Consumer Behavior Research and Virtual Commerce Application Design," *Applied Sciences*, vol. 11, no. 23, 11087. 2021. <https://doi.org/10.3390/app112311087>
2. A. Mhaidli and F. Schaub. "Identifying manipulative advertising techniques in XR through scenario construction," *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems (CHI '21)*, pp1-18, 2021 <https://doi.org/10.1145/3411764.3445253> (Conference Proceedings)
3. B. Heller. "Watching Androids Dream of Electric Sheep: Immersive Technology, Biometric Psychography, and the Law," *23 Vand. J. Ent. & Tech. L.* 1, pp. 1–52, 2021
4. F. Roesner and T. Kohno. "Security and privacy for augmented reality: Our 10-year retrospective," *VR4Sec: 1st International Workshop on Security for XR and XR for Security*. 2021.
5. A. K. Sood and R. J. Enbody. "Malvertising — exploiting web advertising," *Computer Fraud & Security*. vol 2011, no. 4, pp 11–16. 2011. [https://doi.org/10.1016/S1361-3723\(11\)70041-0](https://doi.org/10.1016/S1361-3723(11)70041-0)
6. D. W. Dahl, K. D. Frankenberger, and R. V. Manchanda. "Does It Pay to Shock? Reactions to Shocking and Nonshocking Advertising Content among University Students," *Journal of Advertising Research* vol. 43, no. 3, pp. 268–280. 2003. <https://doi.org/10.1017/S0021849903030332>
7. B. Light, J. Burgess, and S. Duguay. "The walk-through method: An approach to the study of apps," *New Media & Society*, vol. 20, no. 3, pp. 881–900. 2018. <https://doi.org/10.1177/1461444816675438>
8. J. Bailenson. "Protecting Nonverbal Data Tracked in Virtual Reality," *JAMA Pediatr.* vol. 172, no. 10, pp. 905–906. 2018. [doi:10.1001/jamapediatrics.2018.1909](https://doi.org/10.1001/jamapediatrics.2018.1909)
9. C. Allen and V. McIntosh. "Safeguarding the metaverse," *The Institution of Engineering and Technology*. 2022. [Online]. Available at: <https://www.theiet.org/media/9836/safeguarding-the-metaverse.pdf>
10. S. Bloomberg. "Political Advertising in Virtual Reality," *First Amendment Law Review*, 2023. <http://dx.doi.org/10.2139/ssrn.4245908>
11. Federal Trade Commission—Advertising and Marketing [Online]. Available at <https://www.ftc.gov/business-guidance/advertising-marketing/children>
12. L. Wang, H. Wang, R. He, R. Tao, G. Meng, X. Luo, and X. Liu. "MalRadar: Demystifying Android Malware in the New Era," *Proc. ACM Meas. Anal. Comput. Syst.* vol. 6, no. 2, 27 pages. 2022. <https://doi.org/10.1145/3530906>
13. J. Knibbe, J. Schjerlund, M. Petraeus, and K. Hornbæk. "The Dream is Collapsing: The Experience of Exiting VR," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems (CHI '18)* pp. 1–13. 2018. <https://doi.org/10.1145/3173574.3174057>
14. M. L. Fransen, P. W.J. Verlegh, A. Kirmani and E. G. Smit. "A typology of consumer strategies for resisting advertising, and a review of mechanisms for counteracting them," *International Journal of Advertising*, vol. 34, no. 1, pp 6–16. 2015. <https://doi.org/10.1080/02650487.2014.995284>
15. M. A. Martens, A. Antley, D. Freeman, M. Slater, P.J. Harrison and E.M. Tunbridge. "It feels real: physiological responses to a stressful virtual reality environment and its impact on working memory," *Journal of Psychopharmacology* vol. 33, no. 10, pp1264–1273. 2019. <https://doi.org/10.1177/0269881119860156>

Abraham Mhaidli is a PhD graduate from the University of Michigan's School of Information. His research interests include exploring the harms of emerging technologies, such as Virtual Reality, and understanding how to best anticipate and mitigate these harms. Con-

tact him at mhaidli@umich.edu.

Shwetha Rajaram is a PhD student at the University of Michigan School of Information. Her research interests include human-computer interaction, augmented & virtual reality, and privacy & security. Contact her at shwethar@umich.edu.

Selin Fidan Selin Fidan is a Human-Machine Interface Safety Engineer at Stellantis, Auburn Hills, MI, and is interning with the Future of Privacy Forum as an Immersive Technology Policy intern. Selin received her Bachelor of Science in Information from the University of Michigan in 2022. Contact her at selfidan@umich.edu.

Gina Herakovic is an experience design consultant at Slalom. She received her master's degree in Human Computer Interaction from the University of Michigan. Contact her at gherakov@umich.edu.

Florian Schaub is an associate professor of Information and of Electrical Engineering and Computer Science at the University of Michigan. His interdisciplinary research combines privacy, human-computer interaction, emerging technologies, and public policy. Schaub received a doctoral degree in computer science from Ulm University, Germany. Contact him at fschaub@umich.edu.