Original Article

MEDIA INTERNATIONAL AUSTRALIA

Media International Australia
1–15
© The Author(s) 2021
Article reuse guidelines:
sagepub.com/journals-permissions
DOI: 10.1177/1329878X211041670
journals.sagepub.com/home/mia
SAGE

Examining visions of surveillance in Oculus' data and privacy policies, 2014–2020

Ben Egliston
Queensland University of Technology, Australia

Marcus Carter
University of Sydney, Australia

Abstract

Virtual reality – a site of renewed interest for major players in the tech industry – is increasingly one fraught with questions of data capture. This article examines the case of the Facebook owned virtual reality company Oculus and its intensifying privacy and surveillance risks with respect to the data generated and gathered through its devices. To explore the surveillance-centred structures of Oculus, this article examines Oculus' privacy policies from December 2014 (the first version following the company's acquisition by Facebook), and October 2020 (the most recent iteration of the policy). In so doing, we examine these policies as sites of discourse, asking how they frame and afford power and control to Facebook, and position Facebook and Oculus' surveillant aims and logics relative to societal concerns about, and regulations of, data.

Keywords

Data, virtual reality, Facebook, Oculus, privacy policy

Introduction

Virtual reality (VR) has re-emerged in recent years, with significant acceleration following Facebook's 2014 entry into the market through its acquisition of American VR company Oculus. Purchased for US$2BN as one of Facebook's many lucrative post-IPO acquisitions, Oculus has since gone on to form the basis of the mixed and augmented reality (AR) research and development program Facebook Reality Labs (FRL), into which the company has heavily invested. As of 2021, 17% of Facebook's employees are working on AR/VR technology (Hamilton, 2021), and as we argue elsewhere (Egliston and Carter, 2020), Facebook has clear ambitions for using VR as a springboard into further developing embodied and spatial computing interfaces (such as wearables, neural computing and AR) - what CEO Mark Zuckerberg has recently

Corresponding author:
Ben Egliston, Queensland University of Technology, Brisbane, Australia.
Email: ben.egliston@qut.edu.au

referred to as the ’metaverse’. At time of writing, Oculus currently commands a 60% share of the VR hardware market (Lang, 2021), with Oculus’ VR increasingly being adopted beyond its main market focus of entertainment and social networking (e.g. in enterprise settings, see Carter and Egliston, 2021).

In light of Facebook’s ‘surveillance capitalist’ aims and logics (Zuboff, 2019), its status as a key player in the data-driven digital advertising market (Srinivasan, 2018), and in the context of Facebook’s widely publicised improprieties surrounding data privacy and use, a range of emerging scholarship has paid critical attention to Oculus’ data extractive potential (see Egliston and Carter, 2020, Carter and Egliston, 2020a, 2020b; Evans, 2018; Madary and Metzinger, 2016). This is crucial because VR technology is fundamentally reliant upon the capture and processing of various kinds of spatial data. By this, we refer to the way that VR technologies feature increasingly sophisticated capacities to sense the human body and read it as a new paradigm of data – something which has been variously flagged as a privacy concern, for reasons of the data’s granularity (XR Safety Initiative, 2020: 40) and identifiability (Miller et al., 2020). VR also captures and processes various forms of spatial data relating to physical space. Recent forms of VR – such as the Quest and Quest 2 – are reliant upon external cameras and an algorithmic odometry stack in order to sense the position and movement of the device in space (see Saker and Frith, 2020). These data collection capacities raise concerns about the visual and spatial access they provide Facebook to the built environment, the possible insights they provide Facebook into users’ cognition, preference and biases, and the total control Facebook has over their closed Oculus ecosystem (see Egliston and Carter, 2020).

It is in this context of VR working as a data-rich digital sensor, and its backing by Facebook with their surveillance-based business model, this article presents a ‘critical audit’ (following Neville, 2020) of Oculus’ privacy policies – a set of documents outlining stipulations pertaining to privacy, and in particular, data privacy. Our scope is inclusive of documents spanning December 2014, following Oculus’ acquisition by Facebook to October 2020, which saw a major update to the company’s policy documents following numerous corporate announcements by Oculus and Facebook. Rather than focusing on the software license as both a digital and legal mechanism for platform enclosure and control[1] (cf. Sadowski, 2020), in our analysis we were interested in the software license as a site of discourse. By discourse, we mean statements through which particular knowledges are constructed (Foucault, 1970), powerful in shaping perceptions about technology and its role in society (Jasanoff, 2015).

As Neville puts it, corporate license agreements can be ‘interpreted as a discursive formation because they exhibit a generic structure, obfuscating use of legalese, and form of hyper intertextuality’ (2020: 344). The similar ‘terms of service’ (TOS) agreement is discursively constructed or, following Gillespie, ‘designed to protect the provider from as much liability as possible while ensuring it the most discretionary power’ (2018: 31). For van Dijck, while End User License Agreements (EULAs) and TOS *are* legal agreements, they are also discursive mechanisms, control over which rests in the hands of technology owners and providers (2013: 38), where ‘interested parties are engaged in (re)setting the norms for privacy, property, and proper behavior’ (2013: 37) in ways that benefit their economic interests. The privacy policy is in this sense, and as we go on to show through our analysis of Oculus, less a mechanism through which user expectations for (data) privacy are clearly delineated, but rather a discursive device for Facebook to at once position itself for maximal data extraction, while simultaneously appearing as responsive and responsible in light of questions of data privacy.

Taking the privacy policy as a discursive articulation of Facebook’s aims with Oculus, we ask what forms of power and control (particularly those to do with data extraction) are being afforded to Facebook via its VR apparatus, and how are these changing over time? What does Facebook seek to gain from its dominant role as an actor in the VR market? But beyond this, how does

Facebook use the genre of the privacy policy to discursively position itself relative to questions of data capture (and moreover, increasingly widespread concerns about the company's data impropriety)?

In examining the Oculus data privacy discourse, we are interested, on one hand, in how it is an expression of ideology, of corporate ambition, particularly when it comes to data. As Light et al. (2018: 891) note of mobile apps, formal licensing agreements 'may provide information about the ownership and applications of user data'. In the present study, we argue how Facebook's Oculus privacy policies sum up the company's longstanding extractive ambitions, dovetailing with what Srnicek (2017) has called 'platform capitalism' – that is the monopolisation of the global economy by platform-based businesses, many of which are centrally reliant upon data extraction and surveillance. What is articulated through the data and privacy policies, is a vision of how Oculus may operate on the basis of capturing and harnessing user data and 'network effects', to both feed into the refinement of Facebook as an 'advertising platform' (Srnicek, 2017) and the development of future products (and enabling the further expansion of extraction, Srnicek 2017: 98). But the data and privacy policies also, crucially, serve as a discursive technique to create favourable narratives about the company's intentions and to make users compliant with extractive business models, and to mollify investors, critics, and regulators, and create a sense that Facebook is following regulations and best practices.

A 'critical audit' of oculus' privacy and data policies

This article examines 10 Oculus privacy policy documents from December 2014 to October 2020. This includes an analysis of six privacy policies, but also four supplemental privacy related documents – a standalone data collection policy, a third-part developer policy, a California Consumer Privacy Act (CCPA) compliance policy, and a policy for Facebook's expansion of Oculus as enterprise hardware/software (see Table 1). Structurally, earlier privacy policies were longer-form and characterised by legalese, but more recently (particularly in the period 2020 onwards), the company moved to shorter-form and more plain-language policies, and the inclusion of short 'supplemental' policies (e.g. for data use by businesses or content developers). While these are arguably more accessible in wording and length, we found that shorter but multiple documents introduced a greater degree of intertextual relation between documents.

We chose 2014 as the starting point for our data collection as it represents the first privacy policy available following Oculus' acquisition by Facebook. We chose 2020 as the end date for two reasons. First, and most straightforwardly, it was the most up to date iteration of the policy. Second, it represents a major update to the privacy policy pertaining to data use (with the release of a 'supplementary' Oculus data policy in addition to the privacy policy) as well as an expansion of the policy to shift its focus from end users as consumers, to end users as enterprise.

Following Neville's 'critical audit' of the Amazon Echo EULA – which develops a critical discourse analysis approach to a privacy policy's 'legal account of various sociotechnical developments' (2020: 345), we conducted a discourse analysis of Oculus privacy policy documents to provide evidence in support of growing privacy and surveillance concerns. Our approach – focusing on privacy policies covering the use of the Oculus Rift (and Rift S), Go and Quest/Quest 2 devices – focused specifically on discourse relating to data capture and data privacy. Oculus does not provide a changlog of different versions of their privacy policies and license agreements – and as such, it is difficult for both consumers and researchers to track changes made to these licenses and policies. To achieve this in the present research, we made use of the Internet Archive 'Wayback Machine' – a service that enables visiting archived websites, and is particularly useful in enabling scholars to

Table 1. Oculus privacy policies and supplemental privacy policies.

Document name	Document type	Date	Corresponding time period
'Oculus Privacy Policy' (version 1, post-Facebook acquisition)	Privacy policy – general	8 December 2014	2014–2016: post-Facebook acquisition
'Oculus Privacy Policy' (v2)	Privacy policy – general	12 February 2016	
'Oculus Privacy Policy' (v3)	Privacy policy – general	20 May 2018	2018–2019: Facebook growing the 'XR ecosystem', responding to privacy and data regulation (GDPR)
'Oculus Privacy Policy' (v4)	Privacy policy – general	4 September 2018	
'Oculus Privacy Policy' (v5)	Privacy policy – general	27 December 2019	
'CCPA Compliance Policy'	Privacy policy – CCPA specific	1 January 2020	2020–2021: Facebook further responding to privacy and data regulation (CCPA), expanding VR into new settings (workplaces), imagining Augmented Reality futures (building on current VR technologies)
'Oculus Privacy Policy' (v6)	Privacy policy – general	20 May 2020	
'Developer Data Use Policy'	Data policy for third-party Oculus content developers	n.d. May 2020	
'Oculus Supplemental Data Policy'	Privacy policy – data specific	11 October 2020	
'Oculus for business policy' (including 'Oculus for Business Data Processing Addendum')	Privacy and terms of service	11 October 2020	

study 'conceptions of governance' (such as the 'length, complexity and nature of TOS') over time (see Light et al., 2018: 890–891). We downloaded all versions of the privacy policies and license agreements captured by the Wayback machine, and then identified each unique version (through the dates on the documents). To track changes between versions of the policy over time, we used Microsoft Word's compare feature between iterations of policy. The value of comparitive, longitudinal approaches to analysing platform privacy policies has been highlighted previoulsy by studies such as Neville's (2020) examination of Amazon and Katzenbach et al.'s (2021) 'platform governance archive', covering the policies of Facebook, Instagram, Twitter and YouTube.

Our discourse analysis approach to analysing the material involved closely immersing ourselves in the material, such that 'interpretative meanings can crystyalize' (Corrigan, 2018: 2764; on the use of such approaches to study digital media, see Carter and Egliston, 2021; Wilken et al., 2019). As such, our collection and review of the empirical material also involved a process of note taking and drafting of analytic memos. These memos then underwent analysis and a process of open coding (Corbin and Strauss, 2015), where Egliston identified key themes. This was followed by a process of review and discussion with Carter. Following approaches to discourse analysis described by Fairclough (1995), this discussion was sensitised by a review of critical political economic issues (particularly to do with data and platformisation) identified in our literature review and wider studies of VR (see Egliston and Carter, 2020; Carter and Egliston, 2020b).

Findings and discussion

In what follows, we explore the surveillant discourses of Oculus as articulated through Facebook's privacy documents. Our research findings are segmented into three main historical timeframes: (1) the period immediately following Facebook's acquisition of Oculus, (2) the move to mobile virtual reality (MVR) and Facebook's imagination of an 'XR ecosystem' connected with its wider suite of social software, framed in light of the General Data Protection Regulation (GDPR), and (3) Facebook's post-California CCPA treatment of data privacy and its move towards VR for enterprise.

Stage 1: Post-Facebook acquisition (8 December 2014 to 12 February 2016)

The first privacy policy from the post-Facebook acquisition Oculus was effective 8 December 2014. At this point in time Oculus was still relatively autonomous from Facebook (e.g. not requiring Facebook logins). Notably, the policy does not mention Facebook until several pages in. The opening lines of the document, for example, read by referring to 'Oculus VR, LLC', implying a kind of independence in the company – something backed up by then-Facebook-employed Oculus founder Palmer Luckey and CEO Brendan Iribe's assurance to Oculus consumers that 'we're going to continue operating independently [of Facebook]' (Hollister, 2014: n.p.). This changes in later documentation, such as the 2018 privacy policy, which begins by outlining that Oculus is a 'Facebook company', or the 2020 policy, which begins with 'Facebook makes virtual, mixed, and augmented reality hardware and software products … collectively, Oculus products'. Data capture – while extracted from users who agree to the TOS – is framed in terms of what is volunteered ('what you give to us'), including user registration information (e.g. name, email address, phone number, date of birth), transactional data (payment information) and communications with other users.

The 2014 privacy policy – at the end of the section titled 'What kind of information is collected' and throughout the section titled 'How do we use information' (a section that carries into more recent iterations of the privacy policy) make clear Facebook's motives to use Oculus data to generate richer profiles of users (via connecting Oculus data with use of other Facebook owned companies). As it reads:

> We may receive information about you from other companies that are within the family of related companies that are legally part of the same group of companies that Oculus is part of, or that become part of that group, such as Facebook, and may combine that information with other information we collect about you.

The agreement follows on by stating that the information that Facebook collect from Oculus users will be used to 'market to you' as well as to 'improve our services and to develop the virtual reality ecosystem'. Both the 2014 and 2016 privacy policies pay particular attention to the collection of 'spatial data' – that of the body, of the dimensions of the user's play space, and so on. Notably, the 2014 agreement frames data as volunteered (consistent with its framing of data elsewhere): 'When you use our Services, *you may have the option* [emphasis added] of submitting information about your physical features and dimensions'. This tone changes in the 2016 agreement, which simply states that 'Information about your physical movements and dimensions when you use a virtual reality headset' fall under the remit of Facebook's data policy – a framing which is more in line with the Facebook's extractive ambitions.

While critiques of Oculus as a technology of surveillance capitalism are relatively nascent (emerging over the last several years), as we see here the Oculus privacy policy has always made clear

Facebook's ambitions to harvest data from its users (or to combine Oculus user data with other forms of data generated through the Facebook platform). While it has not necessarily always been used as such, Facebook has always discursively framed Oculus as a technology of extraction. This of course makes sense, given the company's acquisition of Oculus not long after successfully adopting and integrating mobile media into the platform. By 2017, most of Facebook's users were mobile users (Goggin, 2014) – and this early and strategic adoption of the mobile provided additional data points (such as location) for the company to connect Facebook users with advertisements through its ad service (see Wilken, 2014). Facebook see clear value in incorporating new technologies into their software ecosystem (see Helmond et al., 2019; Nieborg and Helmond, 2018).

The data-extractive benefits for Facebook – to the company as a platform which provides digital advertisers access to 'eyeballs' of its users (see Srinivasan, 2018) – are clear in these documents. The first, more obvious benefit, is that Facebook may use its Oculus data to further empower the efficacy of its advertising arm, and thus drive up the price it can charge for access to its ad network – a further intensification of an already existing surveillance capitalist marketplace. The second is that its access to 'spatial' VR data rhetorically inspires confidence in the accuracy of Facebook's data-driven ad network, particularly key at a time when critiques of the efficacy of targeted advertising are increasingly common (Hwang, 2020).

Stage 2: A growing XR ecosystem, and the spectre of data privacy regulation (20 May 2018 – 27 December 2019)

The second period we identified began 20 May 2018. This period was characterised by Facebook branching into MVR in early May 2018, and a discursive shift toward discussing a Facebook-owned XR 'ecosystem'. This is characterised by interoperability and flows between XR devices and the wider Facebook platform (see Carter and Egliston, 2020a). It was also marked by the beginning of the European GDPR – arguably the world's most sophisticated and expansive data protection policy. Prior to this moment, Facebook had generally escaped liability for data collection through simply posting its data-use practices in its privacy policy – however, under the GDPR data processing records are required – and compliance with these regulations outlined in a company's TOS.

The concept of the 'XR ecosystem' is first noted in the 20 May 2018 iteration of the privacy policy, with Facebook using 'the information we collect to …develop the XR ecosystem' (coinciding with the company's wider imagination of Oculus as a technology integrated into the Facebook suite of social software at its 'Oculus Connect' conference, see Egliston and Carter, 2020). Notably here, the document specifies the companies that Facebook will potentially share its Oculus data with: Facebook Payments, Atlas, Instagram, Onavo, Moves, WhatsApp, Masquarade and Crowdtangle. The document specifically denotes the ability to 'solicit and analyse input and feedback about our services', to 'identify and address technical issues on our services', to 'conduct and learn from research about the ways in which people use our services', and to 'improve services offered by others, such as third parties that offer content, games, apps and other experiences on our platform'. The idea that Facebook would share its Oculus data with other parts of the company is discursively framed in terms of necessity and positive benefit – 'Facebook…*powers social features* on Oculus' (emphasis added). This shift took place during Facebook's rebrand of Oculus Research to FRL. While Facebook has long maintained ambitions of developing an XR ecosystem – it was FRL that represents a formalisation of this ambition; going on to acquire a number of AR and VR related start-ups in this time, such as Surreal Vision in 2015 (a UK-based 'computer vision' developer, specifically interested in real-time three-dimensional (3D) scene reconstruction, and 'presence and telepresence'), The Eye Tribe (an eye-tracking start-up) in 2016, or CTRL Labs in 2019 (a neural interface start-up).

Data extraction likewise remains a focus of this set of privacy agreements – and much of the language remains unchanged from the previous iteration. A key difference is in the shift from tracking the VR *device*, toward a focus on the potential for tracking the *user*, including biometric data, and toward a more relational, spatial form of tracking to do with the user's environment. The 2018 update notes the capture of 'Information about your environment, physical movements, and dimensions when you use an XR device. For example, when you set up the Oculus Guardian System to alert you when you approach a boundary, we receive information about the play area that you have defined'. While not stated in the license itself – an Oculus blog post accompanying the December 2019 update suggests that data which could be personally identifying is de-identified upon collection. As the blog post states:

> Some data, like positional and movement tracking, is necessary for your Oculus hardware to function properly, but after it's processed for that purpose it's de-identified because we don't need it to be tied to your account anymore

Of course, worth noting here, de-identified information in the present does not mean de-identified in the future. As one study by Miller et al. (2020) showed under experimental settings, based on 5 min of data using a VR system (with all personally identifiable information stripped) researchers could correctly identify using a machine learning algorithm with 95.3% accuracy participants from the study's 511 participant sample. As noted by the journalist Bye (2020), a 2020 Twitter interaction between the Stanford University VR Lab Twitter account (which posted an announcement of Miller et al.'s study) and then-Facebook-postdoctoral researcher Ilke Demir suggests that Facebook had conducted research as early as 2018 revealing that the company had worked out how to identify anonymous VR users through unique motion signatures (Bye, 2020).

This shift in discourse comes several months in advance of Facebook's September 2018 announcement of the Oculus Quest – the company's second wireless, 'mobile' VR platform (released for sale in May 2019). Crucially, as Facebook variously outline in subsequently released technical documentation, the Quest is reliant upon external facing cameras and an algorithmic odometry system to track the position and movement of the device, and to register that position and movement within the software (essentially with the Quest creating an accurate 3D 'map' of the environment around the user). When we consider this development in light of Facebook's data policy covered in this section, space and movement are not only inscribed in the generation of the Quest's 3D map – but potentially in Facebook's data centres and ad networks, and thus a means to further advance the company's surveillance capitalist ambitions.

This second timeframe also saw the addition of policies responding to GDPR guidelines (implemented 25 May 2018). As Facebook summarises in a blogpost accompanying the update: 'In light of the GDPR changes in the EU, we're taking the opportunity to update the global Oculus community about the information we collect and how we use that information'. Notably, the May 2018 license version saw the policy amended to point toward the addition of the Oculus 'My Privacy Center' setting – 'a new, centralized location where you can easily learn about your privacy settings and manage your communications preferences. You'll get access to new tools that let you see the information we've collected that's associated with your Oculus account and easily download a data file of the information you've shared with Oculus so you can take it with you'.

The discourse here encapsulates tenets enshrined in the GDPR, of data protection as a fundamental right. The subject is framed as having a great degree of autonomy over the harvest and storage of their personal data. But despite creating a perception that Facebook is exercising responsibility in their adherence to data privacy laws, the limitations of the GDPR – as expressed in critical legal scholarship, would suggest that despite Facebook's posturing around GDPR adherence, it is something unlikely to limit Facebook's data extractive ambitions (and thus, more than anything, Facebook's posturing discursively constructs the company as a data-responsible actor, particularly when it comes to data harnessed from VR).

Making the case against the GDPR, political economist and legal theorist Salomé Viljoen (2020) argues that the GDPR represents what she calls a 'dignitarian' response to data governance – that is, one that sees the problem with data capture as violating personal dignity. The answer for dignitarian responses like the GDPR is to limit the collection of data, achieved through the implementation of stricter data privacy laws. As Viljoen sees it, a limitation of such approaches is that they conceive data as mediating a 'vertical' relation between the data subject (the user) and a company (the data collector) – seeking to strengthen the user against the collector – generally conceiving of data as something that pertain primarily to individuals (for a similar criticism, see also Couldry and Yu, 2018). But, as Viljoen argues, and many other social scientific accounts of data show, data is not simply about individuals, even if it is extracted from them. The value of Facebook's data capture and highly profitable advertising network is of course based on data in aggregate – and the use of this aggregate data to predict, profile and shape behaviour. Thus, while Facebook has baked in mechanisms for GDPR compliance, such a move must be evaluated with reference to the limitations of the GDPR to actually bring about anything distinct from Facebook's perpetual cycle of data and capital accumulation. In the case of VR, this compliance imposes limited restrictions on what Facebook can collect from their users and do with that data.

Notably, while Oculus has signalled its XR ecosystem's compliance with the GDPR, its relationship to local privacy law in specific European states has been characterised by friction. An emerging example is the case of Germany's national competition regulator's response to Facebook's 2020 decision to require Facebook logins for new Oculus users. Facilitated by Germany's stringent consumer and privacy law, and off the back of a 2019 case by the regulator against Facebook for its internal data-sharing, an investigation is now underway into Oculus' integration into the Facebook ecosystem (during which time Facebook has withdrawn Oculus devices from sale in Germany). While Oculus is pursuant to local law, as their TOS outlines, the extent to which their product coheres with the robust data protection of countries like Germany (and the values of data privacy expressed by German policymakers) is clearly limited. At present, however, it does not appear that this local law is shaping Facebook's (both material and discursive) construction of the XR ecosystem to the extent that the GDPR has.[2]

Stage 3: AR futures, data policy and CCPA compliance, and the future of work (20 May 2020 – present)

The next stage follows on, approximately, from Facebook's 2020 Facebook Connect developer conference. While the main discourse at the conference centred around Facebook's future ambitions for developing AR 'smartglasses' in the vein of Google Glass (see Applin and Flick, 2021; Carter and Egliston, 2020a), the subsequent amendments to the software agreement were centred around (1) further clarifying the use of Oculus data for future product development (including further amendments to comply with data privacy regulations, in this case the CCPA), and (2) Facebook's expansion of VR into new markets, specifically for enterprise use.

The further clarification provided about Oculus' data capture is explained in a new document, the Oculus 'Supplemental data policy' (11 October 2020). Notably, Facebook's relatively straightforward supplemental data policy stands in contrast to both previous iterations of the Oculus license agreements in terms of length. Facebook's data policy in this period focuses more on the use of data to inform further product development. As this policy reads, data will be used:

> to improve and develop aspects of our services, such as voice services and hand tracking. For example, for voice services, we analyze and review your voice commands using human and machine processes to improve, troubleshoot, and train our speech recognition systems. When you enable the hand tracking feature, we collect technical information like hand tracking quality, the amount of time it takes to detect your hands, and the number of pinches you make to improve and troubleshoot this feature.

While this specifies a number of uses of data about the body and its movements, its wording is sufficiently open to include almost anything. For instance, how might the spatial data generated through devices like the Oculus Quest (and its computer vision odometry stack, see Hesch et al., 2019) be a potential source of data to power the company's future AR ambitions, outlined in 2020 as 'Project Aria' (see Applin and Flick, 2021). As Facebook emphasise, Aria's key affordance is contextually and locationally specific annotations of environments. Data from VR and AR devices – which capture data to locate the user within space in granular detail – could as such feed into the development of Aria's spatial maps, and further advance Facebook's pursuit of profit in the AR market.[3]

Notably, data for future product development was covered in a 2020 data privacy policy for third-party Oculus developers. This policy outlines permitted third-party use of developer data, essentially limiting use to improving content via analytics (only if the data is anonymised and aggregate), and explicitly prohibiting uses of data for advertising, sale to third parties, or use 'to perform, facilitate or provide tools for surveillance'. Notably, this policy for developers – which creates a sense of Facebook's responsible governance of its XR ecosystem – is more stringent and clearly defined than Facebook's statements regarding its own use of Oculus data.

Facebook's policy was also updated in the October 2020 license to include a CCPA-compliance statement, entitled 'California Privacy Notice'. 'The California Privacy Notice is for California residents and supplements our Oculus privacy policy. It explains how we collect, use, and share your Personal Information and how to exercise your rights under the California Consumer Privacy Act'. The CCPA is broadly similar to the European GDPR – offering enhanced rights of individual protections and control over one's data (such as rights to access, correct and delete data). While the CCPA is a 'local' law, it applies to Facebook (and many other tech companies) that are based in or trade in California (and the company's intention to commit to the CCPA, as outlined in this policy, is perhaps a result of the size of the California market relative to the previously discussed example of Germany). As the CCPA compliance statement notes, under the CCPA, California resident Oculus users have the 'right to request that we disclose to you the Personal Information we collect, use, or disclose, and information about our data practices'. Further, users have the 'right to request that we delete your Personal Information that we have collected from you'. Notably here, Personal Information is taken to include individually identifiable information rather than that which is taken in aggregate or that cannot be reasonably linked to the user. Indeed, as we argued earlier, an assurance of de-identified data in the present may mean little in the future. Once again, as with Facebook's statements about GDPR compliance, the extent to which CCPA compliance will impose limits on Facebook's extractive business model will likely be minimal.

The second major addition was the 30 March 2020 introduction of the Oculus for Business policy and Oculus for Business Data Processing Addendum. Both of these come at a time where Oculus is expanding the scope of its software and hardware suite beyond entertainment and social networking, which have up until this point been its major focus (see Egliston and Carter, 2020). As Oculus put it on their website, Oculus for Business offers ‘enterprise grade virtual reality’. Unsurprisingly, Facebook’s framing of its enterprise hardware is highly solutionist – framing VR as a means for collaboration, simulation, enhanced efficiency and so on.

As we have written previously (Carter and Egliston, 2021), Oculus has entered into partnerships with numerous VR training simulation companies, as well as numerous retailers in the United States (most notably, and problematically, Walmart) – a further extension of the company’s imagination of Oculus as an ‘everyday’ technology that serves purposes beyond entertainment (see Egliston and Carter, 2020: 8–11). The business agreement makes Oculus modifiable, allowing programmers and developers to go beyond the original designers’ project (cf. Plantin et al., 2018) – as we see with the development of Oculus based training software by companies like STRIVR and TaleSpin.

The license agreement outlines stipulations for businesses, as well as parties using the service (i.e. employees, etc.) pertaining to data processing. As it reads:

> we collect the following kinds of information [including device information and information about how users interact with the hardware and software, as the policy notes elsewhere] on behalf of your Organisation when you, your colleagues or other users access or use the Products, and this information will be available to your Organisation.

Here, we see that Facebook’s move is likely not one just about expanding into to new markets, supplying the company an additional revenue stream in terms of the cost of an enterprise headset (US$799), nor necessarily to solidify their position in society (cf. Sadowski, 2020: 569). Rather, it provides a further means to extract data, doing so in a way that provides a workaround to traditional requirements of consent for end users (where consent is given on the basis of one’s workplace’s decision to implement the technology).

While the agreement provides clear insight into Facebook’s surveillance capitalist ambitions, a further issue lies in the relationship between Oculus, employers and third parties (such as third-party enterprise software providers). As the agreement for enterprise use reads:

> Your Organisation may configure the Products to allow you to interact with third-party content, apps and other experiences through the Products. Third-party content providers may also collect information from you directly through the experiences they provide. Please note that any information shared with these (or other) third parties will be subject to those third parties’ own privacy policies, not this privacy disclosure.

Third party policies – such as those of companies like STRIVR, an enterprise training company specialising in VR software and ‘learning analytics’ – note their ownership of data generated in the use of its software (Carter and Egliston, 2021). Further to this, STRIVR’s datasets will supposedly be used to develop learning models and evaluation tools – things which do not just affect the individual user but other users of STRIVR’s software. As we argue elsewhere, this is an urgent political economic concern and something with the potential to exacerbate workplace inequality (Carter and Egliston, 2021). Thus, the licensing agreement’s affordance to third party platform complementors creates the potential for further ‘horizontal’ data relations, per Viljoen, where data relations and flows are not just between user and platform, but between user and other users – a kind of relation not protected under the highly individualised EULA (and the highly individualised laws with which the EULA is framed in response to).

Enterprise use – at once a way to further the ‘everyday imaginary’ (see Egliston and Carter, 2020) of Oculus (that is, as a technology taken up in everyday life, beyond niche purposes like gaming), and as a means of advancing Facebook's data-extractive ambitions – as shown through both Facebook and their complementors, highlights the failures of the license agreement to protect users beyond the context of the consumer, and moreover, highlight the failures of consumer-rights focused data privacy mechanisms like the GDPR (van Dijck et al., 2019) and the need for those that focus on political economy.

Conclusions

This article has provided an account of Oculus' privacy policies – from December 2014 to October 2020. Our aim has been to contribute a political economic account of the surveillance centred nature of Oculus; a perspective that Oculus and VR has generally enjoyed cover from, perhaps due to VR often falling under the auspices of benign digital play. In so doing, we have explored what protections users are afforded through these privacy policies, and what provisions are granted to Facebook for data capture. While more recent iterations of the agreement provide a greater degree of specificity in terms of data captured, the agreement's often vague language and open-endedness affords much to Facebook. Further, we note that due to the growing spectre of regulation, Facebook's hand has been forced in engaging with the language of data regulation – statements about compliance with the GDPR and CCPA characterising more recent documents. Yet as we note, in line with critical legal scholarship, such regulations are largely ineffectual at dealing with the very issue that is central across Facebook's data collection practices outlined or alluded to in its policies– that Oculus is simply just another data extractive mechanism for Facebook.

We believe our analysis of Oculus' privacy policies contributes to existing studies of how Facebook has sought to normalise its VR and XR ambitions through its discourse at yearly developer conferences, which stress both the promise of the medium as well as Facebook's commitment to privacy-related best practices (see Egliston and Carter, 2020). More generally, we believe it contributes to a much wider literature on the discursive construction of mixed reality technologies, which have paid little attention to data to privacy policies (Chesher, 1994; Harley, 2020; Heemsbergen, 2021; LaRocco, 2020; Liao, 2016; Nakamura, 2020). Beyond VR and XR, we believe this analysis to contribute broader attempts to understand how Facebook discursively positions its data-capture ambitions relative to policy and critique (cf. Haupt, 2021; Hoffmann et al., 2018; Rider and Murakami Wood, 2019).

While this article has focused on privacy policies for Facebook's currently existing suite of VR technologies, it worth noting the value of critique of the company's policies pertaining to more speculative XR research and development, such as with Aria. In 2020, following the announcement of Aria, Facebook released a set of 'responsible innovation principles' – which recent work by Applin and Flick (2021) critiques for its hollowness, and doing little more than creating a veneer of best practice. Studying these policies is important, even though they do not relate to currently existing technologies and present a means to challenge potentially ethically problematic internal research (as we have seen with Facebook's previous 'emotional contagion' study).

Future work might productively explore how these Oculus privacy policies are navigated by users, or their attitude toward them (as with studies on dating app and social media moderation policies in Duguay et al., 2020). Oculus' license agreement when accessed in the software – much like those of other digital platforms – takes the form of a clickwrap agreement, that is where signing up to the service simply requires ticking a box that the user agrees to the company's terms. While the GDPR has pushed for more concise consent agreements, clickwraps have been heavily critiqued– such as by Obar and Oeldorf-Hirsch (2018, 2020) as a mechanism for quickly moving users into consumption, and essentially circumventing consent. Indeed, as we found in our earlier study of everyday individuals' perceptions of Oculus (Egliston and Carter, 2020), privacy was a recurrent and well-reasoned concern about an encroaching, Facebook-backed VR future. As Facebook only further invest in research and development capacities for spatial computing, and in large part VR, and with the Quest 2 becoming the first VR system adopted at significant scale, scholarship tracking the implications of Oculus' surveillance centred business model will be needed.

Declaration of conflicting interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The authors received no financial support for the research, authorship and/or publication of this article.

ORCID iDs

Ben Egliston https://orcid.org/0000-0002-7878-7208
Marcus Carter https://orcid.org/0000-0002-4866-4928

Notes

1. The privacy policy is important because in order for prospective Oculus users to use the hardware and software, they must agree to the terms presented in the privacy agreement (by clicking agree to an EULA). EULAs are unilateral agreements (specifically, private contract law agreements) between the software provider and the user. Much critical writing has emerged in recent years on the software license as it pertains to data. For legal scholars of data like Viljoen (2020) and Waldman (2019) consent-based mechanisms for permitting data collection – such as license agreements – are largely insufficient in enforcing data protections, and do little more than prevent liability for, and empower companies in data collection. Such agreements as Viljoen suggests often couch data in highly individualised terms, for instance, when of course the power of data lies in its mobilisation in aggregate. Others have suggested that license agreements discourage genuine user engagement with questions of data privacy due to their length and complexity (see Reidenberg et al., 2015; Mcdonald and Cranor, 2008; Obar and Oeldorf-Hirsch, 2018). Beyond its legal definition, software licenses have been framed by critical political economists as a mode of control, and increasingly an apparatus for the interests of platform and data capitalism. As writers like Sadowski (2020) and Komljenovic (2021) suggest, the EULA is a mechanism for locking the user in a 'rentier' relationship – more often than not permitting the control and constant extraction of data 'rents' from the user. In this sense, these agreements protect the interests of powerful actors in the tech sector, rather than operate as a legitimate mechanism for protecting privacy rights and preventing the injustices of data capitalism.
2. There are a number of potential factors here. While Facebook has not explicitly stated it, it may be more likely to adhere to regulations like the GDPR due to the high corporate fines for breaches. Facebook may also simply see the German market as not large or profitable enough to walk back its login requirements.
3. Notably, in September 2020 along with the announcement of Aria Facebook released their principles for responsible innovation in AR development. While the analysis of these documents is beyond the scope of this article, their discourse has been analysed elsewhere in Applin and Flick, 2021.

References

Applin S and Flick C (2021) Facebook's Project Aria indicates problems for responsible innovation when broadly deploying AR and other pervasive technology in the commons. *Journal of Responsible Technology*. 5: 1–15. Epub ahead of print. DOI: 10.1016/j.jrt.2021.100010.

Bye K (2020) So @StanfordVR published research…. Retrieved from https://twitter.com/kentbye/status/1317212859852484608.

Carter M and Egliston B (2020a) Facebook's virtual reality push is about data, not gaming. *The Conversation*. Available at: https://theconversation.com/facebooks-virtual-reality-push-is-about-data-notgaming- 145730.

Carter M and Egliston B (2020b) *Ethical implications of emerging mixed reality technologies*. Socio- Tech Futures Lab: University of Sydney. Available at: https://ses.library.usyd.edu.au/bitstream/handle/2123/22485/ETHICAL IMPLICATIONS.pdf.

Carter M and Egliston B (2021) What are the risks of virtual reality data? Learning analytics, algorithmic bias and a fantasy of perfect data. *New Media & Society* 1–20. Epub ahead of print. DOI: 10.1177/14614448211012794.

Chesher C (1994) Colonizing virtual reality: Construction of the discourse of virtual reality. *Cultronix* 1(1): 1–27.

Corbin J and Strauss A (2015) *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*. Thousand Oaks, CA: Sage.

Corrigan T (2018) Making implicit methods explicit: Trade press analysis in the political economy of communication. *International Journal of Communication* 12: 2751–2772.

Couldry N and Yu J (2018) Deconstructing datafication's brave new world. *New Media and Society* 20(12): 4473–4491.

Duguay S, Burgess J and Suzor N (2020) Queer women's experiences of patchwork platform governance on Tinder, Instagram, and Vine. *Convergence* 26(2): 237–252.

Egliston B and Carter M (2020) Oculus imaginaries: The promises and perils of Facebook's virtual reality. *New Media & Society*. Epub ahead of print. DOI: 10.1177/1461444820960411.

Evans L (2018) *The Re-Emergence of Virtual Reality*. New York: Routledge.

Fairclough N (1995) *Critical Discourse Analysis: The Critical Study of Language*. New York,, NY: Routledge.

Foucault M (1970) *The Order of Things: An Archaeology of the Human Sciences*. London: Routledge.

Gillespie T (2018) *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions That Shape Social Media*. New Haven: Yale University Press.

Goggin G (2014) Facebook's mobile career. *New Media & Society* 16(7): 1068–1086.

Hamilton I (2021) Nearly 20% of Facebook's employees are working on AR/VR. Retrieved from https://uploadvr.com/facebook-employees-2021/.

Harley D (2020) *The politics of consumer VR: Framing contemporary virtual reality*. Unpublished doctoral thesis, York University, Canada. Retrieved from https://yorkspace.library.yorku.ca/xmlui/bitstream/handle/10315/38266/Harley_Daniel_E_2020_PhD.pdf.

Haupt J (2021) Facebook futures: Mark Zuckerberg's discursive construction of a better world. *New Media and Society* 23(2): 237–257.

Heemsbergen L, Bowtell G and Vincent J (2021) Conceptualising augmented reality: From virtual divides to mediated dynamics. *Convergence*. Epub ahead of print. DOI: 10.1177/1354856521989514.

Helmond A, Nieborg D and van der Vlist F (2019) Facebook's evolution: Development of a platform-as-infrastructure. *Internet Histories* 3(2): 123–146.

Hesch J, Kozminski A and Linde O (2019) *Powered by AI: Oculus Insight*. Retrieved from https://ai.facebook.com/blog/powered-by-ai-oculus-insight/.

Hoffmann A, Proferes N and Zimmer M (2018) "Making the world more open and connected": Mark Zuckerberg and the discursive construction of Facebook and its users. *New Media and Society* 20(1): 199–218.

Hollister S (2014) Oculus founder says Facebook deal will make virtual reality cheaper and better. Retrieved from https://www.theverge.com/2014/3/25/5547884/interview-oculus-founder-says-facebook-deal-will-make-virtual-reality.

Hwang T (2020) *Subprime Attention Crisis: Advertising and the Time Bomb at the Heart of the Internet*. Farrar, Strauss; Giroux.

Jasanoff S (2015) Future imperfect: Science, technology, and the imaginations of modernity. In: S Jasanoff and S Kim (eds) *Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power*. Chicago, IL: University of Chicago Press, 1–34.

Katzenbach C, Magalhães JC, Kopps A, et al (2021) *The Platform Governance Archive (PGA).* DOI: 10.17605/OSF.IO/XSBPT.

Komljenovic J (2021) The rise of education rentiers: Digital platforms, digital data and rents. *Learning, Media and Technology.* Advanced online publication. DOI: 10.1080/17439884.2021.1891422.

Lang B (2021) Zuckerberg: Quest 2 'on track to be first mainstream VR headset', Next Headset Confirmed. Retrieved from https://www.roadtovr.com/zuckerberg-quest-2-mainstream-vr-headset-facebook-q4-2020-earnings/.

LaRocco M (2020) Developing the 'best practices' of virtual reality design: Industry standards at the frontier of emerging media. *Journal of Visual Culture* 19(1): 96–111.

Liao T (2016) Mobile versus headworn augmented reality: How visions of the future shape, contest, and stabilize an emerging technology. *New Media and Society* 20(2): 796–814.

Light B, Burgess J and Duguay S (2018) The walkthrough method: An approach to the study of apps. *New Media and Society* 20(3): 881–900.

Madary M and Metzinger T (2016) Real virtuality: A code of ethical conduct. Recommendations for good scientific practice and the consumers of VR-technology. *Frontiers in Robotics and AI* 3(3): 1–23.

Mcdonald A and Cranor L (2008) The cost of reading privacy policies. *I/S: A journal of Law for the Information Society* 4(3): 543–568.

Miller MR, Herrera F, Jun H, et al. (2020) Personal identifiability of user tracking data during observation of 360-degree VR video. *Scientific Reports* 10: 1–10.

Nakamura L (2020) Feeling good about feeling bad: Virtuous virtual reality and the automation of racial empathy. *Journal of Visual Culture* 19(1): 47–64.

Neville S (2020) Eavesmining: A critical audit of the Amazon Echo and Alexa conditions of Use. *Surveillance and Society* 18(3): 343–356.

Nieborg D and Helmond A (2018) The political economy of Facebook's platformizaiton in the mobile ecosystem: Facebook Messenger as platform instance. Media. *Culture and Society* 41(2): 196–218.

Obar J and Oeldorf-Hirsch A (2018) The clickwrap: A political economic mechanism for manufacturing consent on social media. *Social Media and Society* 4(3): 1–14.

Obar J and Oeldorf-Hirsch A (2020) The biggest lie on the Internet: Ignoring the privacy policies and terms of service policies of social networking services. *Information, Communication and Society* 23(1): 128–147.

Plantin J-C, Lagoze C, Edwards P, et al. (2018) Infrastructure studies meet platform studies in the age of Google and Facebook. *New Media and Society* 20(1): 293–310.

Reidenberg J, Breaux T, Cranor L, et al. (2015) Disagreeable privacy policies: Mismatches between meaning and users' understanding. *Berkeley Technology Law Journal* 39: 1–36. Retrieved from. http://ir.lawnet.fordham.edu/faculty_scholarship/619.

Rider K and Murakami Wood D (2019) Condemned to connection? Network communitarianism in Mark Zuckerberg's "Facebook Manifesto". *New Media and Society* 21(3): 639–654.

Sadowski J (2020) The internet of landlords: Digital platforms and new mechanisms of rentier capitalism. *Antipode* 52(2): 562–580.

Saker M and Frith J (2020) Coextensive space: Virtual reality and the developing relationship between the body, the digital and physical space. Media. *Culture and Society* 41(7–8): 1427–1442.

Srinivasan D (2018) The antitrust case against Facebook. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247362.

Srnicek N (2017) *Platform Capitalism.* New York, NY: Polity.

Van Dijck J (2013) *The Culture of Connectivity.* Oxford, UK: Oxford University Press.

Van Dijck J, Nieborg D and Poell T (2019) Reframing platform power. *Internet Policy Review* 8(2): 1–18. DOI: 10.14763/2019.2.1414.

Viljoen S (2020) Democratic Data: A Relational Theory For Data Governance. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3727562.

Waldman A (2019) Privacy Law's False Promise. Wash U. L. Rev. Retrieved from https://openscholarship.wustl.edu/law_lawreview/vol97/iss3/7.

Wilken R (2014) Places nearby: Facebook as a location-based social media platform. *New Media and Society* 16(7): 1087–1103.

Wilken R, Burgess J and Albury K (2019) Dating apps and data markets: A political economy of communication approach. *Computational Culture a Journal of Software Studies* 7(7): 1–26.

XR Safety Initiative (2020) *The XRSI Privacy Framework version 1.0*. Retrieved from https://xrsi.org/publication/the-xrsi-privacy-framework.

Zuboff S (2019) *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.