Data protection challenges for virtual reality applications

Emil Albiñ Henriksson*

Abstract: Virtual reality technologies necessitate the collection and processing of more – and more intimate – personal data than other media. This gives rise to some particular considerations under data protection regulations and not least the EU General Data Protection Regulation. The aim of this article is to explore these characteristics particular to VR and to identify some of the issues that these might give rise to under the GDPR.

Keywords: virtual reality, data protection, GDPR, personal data, privacy, VR

1. Introduction

In this article the term virtual reality (VR) is used to designate immersive experiences enabled primarily by the use of VR headsets. VR content is not limited to video games; music videos, live sports and films can be experienced using a VR headset.

VR technology dates back to the mid-twentieth century and Sega and Nintendo released consumer VR products already in the 1990s. However, technological advances over the last few years have enabled much more advanced VR equipment, which provide a vastly improved experience in comparison to previous consumer VR efforts.

While commercial uptake might have been slower than forecasted, VR is gaining momentum. It is now more than five years since Oculus first announced its Kickstarter campaign for the Oculus Rift headset and around two years since the Rift and the HTC Vive were launched to consumers. Although several other VR headsets have since been launched or at least promoted we are still waiting for a second generation of headsets. In the meantime however, significant price cuts have been made, and wireless options have been introduced; two key steps that might convince previously hesitant consumers to take the leap. Combined with the announcement of several AAA titles designed for VR, there is certainly good reason to be optimistic about 2018. Nonetheless, it might be too early to know for sure if VR will break into the mainstream this time around.

More certain is the fact that the EU General Data Protection Regulation (the ‘GDPR’)¹ became applicable on 25 May 2018, and that this regulation will be highly relevant to most anyone active within the field of VR.

2. Personal data and VR

VR technology presumes the collection and processing of large amounts of personal data. Granted, collection and processing of significant volumes of personal data in, for example, gaming is nothing new and neither is the collection and processing of location data on smartphones and other devices. It is certainly a legitimate question then if the challenges that data protection and privacy regulations may present to VR technologies really differ from the challenges already present in video-gaming and for technology in general. Arguably, for three interrelated reasons, the challenges are new.

First, VR equipment collects new types of data as compared to playing a non-VR game or watching non-VR content. The second reason is the fact that VR offers quite an extraordinarily immersive and even visceral experience. It can trigger your fear of heights or prompt you to actually/physically jump out of the way to avoid an object coming at you. This trait of VR experiences might very well affect how questions of privacy are viewed. A third reason is that our behaviours in VR might prove to be much more similar to how we act in the real world than what currently is the case in the digital realm. This might entail that collection and

* Senior Associate at Mannheimer Swartling.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the

processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

processing of data within a VR context is more akin to a very intimate surveillance in real life than to current processing in the digital realm.

2.1. One: the data collected

VR technologies, in particular higher end headsets such as Oculus and HTC Vive, collect data on physical movements and dimensions of the user, including for instance the direction, speed and angle of the user's hand motion. Other examples include determining the distance between a person's eyes and the relative height of the headset in order to provide an immersive and comfortable experience. In essence the personal data captured is much more intimate than with a normal game.

On the horizon is further processing, for example to enable eye tracking and tracking of facial gestures. The latter especially has been posited as vital for the social aspects of VR. Oculus has already demonstrated the ability to express emotions through facial gestures. Although this was achieved by use of controllers rather than facial tracking, real facial tracking is likely not far away. As an example, UK company Emteq is developing a system that can track users' facial expressions and emotions using sensors on the inside lining of a VR headset. The Emteq sensor reads electrical muscle activity, heart-rate, skin response, eye movement detection and head position.

Looking further into the future, technological advances will likely enable processing of even more data and there are, for instance, already applications out there with EEG sensors. We remain in the early stages of this new generation of VR technologies, but we can already see that collection and processing of personal data of a more intimate nature than before are driven by these new technologies.

2.2. Two: the immersiveness of VR

The revolutionary immersiveness offered by high-end VR might also have an impact on data protection. Because it is a technology that currently receives quite a lot of attention both users and other stakeholders, including legislators, are watching this space closely and much has already been written about VR and privacy. As an example, there was significant user backlash in relation to the Oculus privacy policy and the always

on service that was installed together with the Oculus application. Of particular concern was the fact that the policy allowed sharing the data within the Facebook group of companies as well as to third parties. This even prompted US Senator Al Franken to send an open letter to Oculus, to which Oculus responded in some detail.²

It appears likely that the main driver behind such concerns has been the nature of the personal data captured, coupled with the data-driven nature of the companies involved, such as Facebook and Google. However the fact that our VR-game experiences feel so much more real than in non-VR games might in itself mean that we feel more strongly about how our personal data is used.

Game telemetry might prove to be a good example of this aspect. Most users appear to find rather innocuous the collection and analysis of game telemetry for the purposes of improving the in-game experience, for instance by redesigning a part of a level where a lot of players get stuck. However if game telemetry also comes to include data on our own physical movements and properties, such processing might feel more intrusive.

2.3. Three: moving our real-life behaviours to VR

A further development of this would be if and when we come to associate more closely with our virtual avatars. Because of the immersive and lifelike nature of VR experiences, in particular if combined with body scanning technologies to create 3D replicas of our real selves, the border between our physical and virtual selves might become somewhat less distinct, in a way which goes far beyond that which is present in virtual worlds such as Second Life.

If users identify closely enough with their virtual avatars and part of their lives are even lived out in virtual reality, we are likely to see much more concern over any tracking of what we do in these virtual spaces, as it would enable monitoring of activities and behaviours that (for most people) have previously been confined to the real and mostly unmonitored world.

Another related issue that has already reared its ugly head is that of trolls and cyber bullying. It is important that developers are proactive in this field, certainly more than social media platforms have been in their early

² In the letter, the senator asked whether the collection of location information, as well as users' physical movements and dimensions, is necessary for Oculus to provide its services, and whether the information is shared with any other parties or used for any other purposes. He further asked questions pertaining to data retention and information security. The letter is no longer

available at www.senate.gov. At the time of writing it can be found at <https://www.documentcloud.org/documents/2796548-160407OculusLetter.html>, accessed 30 January 2018. Oculus' response can be found at <https://cdn.uploadvr.com/wp-content/uploads/2016/05/OculusResponseFranken.pdf>, accessed 30 January 2018.

days, first and foremost to ensure that peoples' VR experiences are positive and that the inevitable negative experiences do not come to overshadow the amazing possibilities the technology offers. As with age ratings, where the nature of VR should arguably be accounted for as well, a lack of satisfactory self-regulation in this field may lead to calls for legislative actions which could have a negative impact on the development of VR.

The game QuiVr provides an interesting example. After an article about sexual harassment in the game³ quickly went viral the developers took swift action which they further built upon over time.⁴ The first step was to modify the feature of a personal bubble that already existed, which made a user's hands disappear when they came to block the view of the other user, to include the entire avatar. Interestingly they did not stop there. The developers realized it was not enough to take purely passive and reactive actions to stop harassment. Instead they enabled the activation of the personal bubble with a sort of power gesture, which sends out a ripple force field dissolving any nearby player from view, at least from that user's perspective, giving the user a safety zone of personal space. The developers proposed applying this concept as a single, cross-platform and cross-game action that players can rely on as their call to a safe space. The popular social space Rec Room provides similar functionality and has a clear code of conduct regulating player behaviour.

A further example would be VR as a social media platform. Today we are, or at least feel, more in control of what personal data we share on social media. But when social media moves into VR everything we do and say while in that space can be captured.

Which brings us to the third reason: The life-like nature of the experiences VR can offer may prompt the users to treat VR experiences differently from instant messaging or similar applications and more like real life behaviours. The closest comparison might be to existing virtual social spaces such as Second Life, but VR has the potential to offer a viable option for behaviours/activities that for most people have so far been the preserve of real/physical life.

There are VR applications that allow a group of friends to gather in a virtual cinema to watch a (non-VR) movie together or to explore a city or a museum.

Users could conceivably go shopping together in virtual malls (e-commerce is certainly no stranger to augmented reality and there are already VR shopping alternatives⁵) or watch live sports. It appears plausible that users will be liable to share more information in the (virtual but life-like) company of their friends than most people do online today and that the collection and processing of such information warrant greater concern than digital behaviours more generally.

3. Data protection in VR and the GDPR

Discussions about the GDPR have to some extent been focussed on the high cap for sanctions set by the regulation. While highly relevant, not least because it may prompt more case law on personal data issues, there are a few other aspects that may be of particular relevance for VR.

3.1. VR data as biometric data

In the new regulation the concept of biometric data is defined as (Article 4(14) of the GDPR):

personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic [i.e. fingerprints] data.

It is conceivable that some of the data collected in VR will constitute biometric data. As an example, studies have shown that a person can be identified by his or her walking gait⁶ and facial scans would constitute biometric data. Eye tracking might also constitute biometric data.⁷

This distinction is important since biometric data is considered as sensitive data and thus processing of such data is more strictly regulated. However it is important to note that processing of biometric data is only subject to the stricter requirements in the regulation if it is processed (Article 9(1) GDPR) 'for the purpose of uniquely identifying a natural person'.

Consequently it should, as a rule, be possible to steer clear of these stricter requirements. That being said, it is

3 <https://medium.com/athena-talks/my-first-virtual-reality-sexual-assault-2330410b62ee>, accessed 30 January 2018.

4 See <https://uploadvr.com/dealing-with-harassment-in-vr/> for a post written in response to the article by Henry Jackson one of the developers of QuiVr, accessed 30 January 2018.

5 A. Hines, 'Virtual retail-ity The strange, lonely world of virtual shopping in China' <https://news.vice.com/story/alibaba-vr-shopping-buy-singles-day>, accessed 4 February 2018.

6 See <https://www.wired.com/2011/09/walking-biometric-identification/>, accessed on 31 January 2018. See further Damasevicius, Maskeliunas, Venčkauskas, and Woźniak, 'Smartphone User Identity Verification Using Gait Characteristics' [2016] *Symmetry* 8(10): 100.

7 B. Ravi, 'Privacy Issues in Virtual Reality: Eye Tracking Technology', [2017] *Bloomberg Law Privacy and Security Law Report* <https://www.alston.com/en/insights/publications/2017/07/privacy-issues-in-virtual-reality>, accessed 4 February 2018.

important to note that biometric data is one area where there may be additional conditions imposed in specific member states (Article 9(4) GDPR), meaning that this issue should be monitored closely. It may also be the case that any breaches are judged more severely if processing of biometric data is involved.

3.2. Public perception of processing in VR

Another factor, as discussed above, is that public perception of data processing in a VR context may be different than in a non-VR context. With the example of game telemetry given previously, it may very well be that both the new categories of personal data collected and the real-life nature of the experience prompt users to express much greater concern over game telemetry than what has previously been the case.

From a purely legal perspective this might not have that great an impact directly but if such processing is considered as much more intrusive, there might in practice be a greater risk that users or even supervisory authorities scrutinize such processing more closely. As an example, the Swedish Data Protection Board often focuses on one specific sector at a time (e.g. the health-care sector and the banking and finance sector).

Furthermore, public perception is highly relevant under the GDPR since individuals, alone or acting as a group, are granted capabilities of seeking remedies of any breaches of the regulations.⁸ It can also potentially affect the assessment under several provisions where the nature of the data processed is weighed in.

3.3. Virtual privacy and legal grounds for processing

Related to the issue of public perception is the question whether expectations for a sort of virtual privacy will have effects on how we should structure our data processing. In particular there are several aspects that may make reliance on user consent a less viable proposition.

First, consent might not be considered as freely given if the provision of a service is conditional on consent to the processing of personal data that is not necessary for the performance of that service (see Article 7(4) GDPR). Much of the data described in the above certainly appear to be necessary for enabling the VR experience but there might be a question of where that line is drawn. Is game telemetry for instance necessary for the provision of a game? Arguably this collection is part and parcel of

providing the game but the opposite stance cannot be ruled out.

The second aspect is the introduction of the principles of privacy by default and by design. If user consent is the legal basis then it might be necessary to have users actively opt in to each type of processing, e.g. for game telemetry purposes, rather than having an opt-out model. If too few users opt in, data quality and usefulness will of course be impaired.

A related issue is processing for advertising purposes. Processing personal data for advertising purposes is not – strictly speaking – necessary for providing the service and so the question might arise whether access to a game or other VR content can be conditional upon consenting to processing for advertising purposes. According to Opinion 06/2014 of WP29,⁹ the term ‘necessary for the performance of a contract’ needs to be interpreted strictly. The burden of proof is on the controller. Based on the recent Guidelines on Consent under Regulation 2016/679 (WP259), offering a paid ad-free version alongside a free ad-supported version would not resolve the issue (assuming that personal data is processed in order to serve the ads). It might be possible to offer one version with personalised ads alongside a version with generic ads that require no processing of personal data, if both services are deemed to be genuinely equivalent. Lacking relevant case law, it is too early to tell how strictly the requirement of genuine equivalency will be interpreted.

This is of course an issue outside the VR context as well but VR offers particularly interesting opportunities for advertisers since it is possible to assess in greater detail how long a user is viewing an ad and potentially even the physical reactions of that user to the relevant ad. As stated previously, the immersive nature of VR might further mean that users consider more intrusive processing in VR for advertisement purposes. Consequently, this is an area where legal developments should be monitored.

3.4. Personal data of children

Processing of the personal data of children is more sensitive in many jurisdictions. Generally speaking it is difficult to know whether a user is a child or not and most of the time we are relying on the user to confirm his or her age or that parental consent is at hand.

However if a data controller has access to information about the user’s height and other physical characteristics

⁸ See Chapter VIII of the GDPR.

⁹ The working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995.

it could perhaps be argued that at least for certain non-borderline cases the data controller has the data necessary to infer that a user is a child.

A scenario where VR developers are obligated to take active and burdensome measures to figure out whether a user might be under a certain age does not appear near at hand, and just basing this on height would be quite problematic. However, again, this might be an area to keep one's eyes on.

4. Conclusion

The new generation of virtual reality technologies already offer extraordinary experiences and the pace of development is high; we are continually astounded by what it can offer. VR technology will likely face many legal challenges and there has already been high-profile litigation in this area.¹⁰ Although many of the challenges will likely be similar to what has been seen with other emerging technologies, data protection is one area where the nature of VR is likely to require some particular thought. Further, the fact that the emergence of VR coincides with the GDPR becoming applicable, a regulation which gives rise to many new questions in itself, adds to the complexity of developing data protection compliant VR technologies and applications.

As described above, the collection of categories of personal data not previously collected in non-VR

applications is necessary for enabling immersive (and comfortable) VR experiences. At the same time this very immersiveness might on the one hand mean that users are liable to share more information about themselves, in part because users enjoy activities previously only enjoyed in real life, while on the other hand it might also mean that they will be much less comfortable with the collection and processing of the vast amounts of data that we have slowly become used to in the digital realm.

This development is concurrent with the introduction of a stricter data protection regulation in the EU and, arguably, a greater public awareness of these issues. The last aspect is important as the remedies for individuals under the GDPR might compensate for the possible lack of sufficient funding that many of the national data protection authorities have raised as potentially impacting the efficiency of enforcement.¹¹

The increased processing of personal data, together with the potential for increased user concern, coupled with the introduction of stricter regulations including new means for individual redress and higher sanctions, all point to VR as potentially being one of the most interesting domains in relation to data protection in the next few years (the 'internet of things' being another one¹²). There is every reason then for anyone developing VR technologies and applications to think long and hard about compliance with data protection regulations.

10 See *Total Recall Technologies v. Palmer Luckey and Oculus VR LLC, as successor-in-interest to Oculus VR Inc.*, No. 15-2281, N.D. Calif. See further *Zenimax Media Inc. and Id Software LLC, v. Oculus VR, Inc., Palmer Luckey, Facebook, Inc, Brendan Iribe, and John Carmack*, 3:14-cv-1849, N.D. Texas. See also *Zenimax Media Inc. and iD Software LLC, v. Samsung Electronics Co., Ltd., Samsung Electronics America, Inc., and Samsung Telecommunications Of America*, 3:17-cv-01288-D, N.D. Texas.

11 D. Meyer, 'Some EU DPAs increasingly desperate for GDPR resourcing' <https://iapp.org/news/a/some-eu-dpas-increasingly-desperate-for-gdpr-resourcing> accessed 4 February 2018.

12 And as has happened in relation to IoT devices, it does not appear far-fetched that state interests, most prominently as represented by law enforcement and national security more generally, will also crash with data protection in a VR context.