

Written evidence submitted by Winter (DDA0034)

Introduction: I am a computer science student interested in the privacy aspects of videogames and their compliance towards GDPR.

Purpose for submitting evidence: To highlight the data collection in games for health and how the data generated from these games for a medical purpose can pose a privacy issue.

The video game industry is plagued with numerous data breaches, fines applied to organisations for breaches, and big tech changes to surveilling consumers. “With users, developers, and the wider public being mainly focused on their features and entertainment value, it has been widely overlooked that video games constitute a substantial threat to consumer privacy.” [3]

Many commercial games fail to offer a sufficient explanation as to what data collected is necessary for the function of the game, what data is necessary for the functioning of the company, and what data is optional data. Opt out of non-essential data collection is rarely seen with commercial games preferring to adopt an “all in or not at all” solution for user privacy options. Tracking and profiling of anonymous users can be exploited for questionable purposes. Full name, email address, social media profile, postal address, credit card details, and other identity-related information are just some of examples of data a game may collect about its players. Most of this information is easily obtained during sign-up to a video game or gaming platform [1]. Employ tracking technologies similar to what can be found on websites and mobile applications. This includes browser fingerprinting and cookies. Enabling the re-identification of individual users and tracking of their activities across different games. This can occur even when they are not logged in [5]

Numerous companies in the video game industry, including market-leading players, have been involved in major data breaches and been accused of sharing personal data with third parties. December 2021 saw a data breach of Ubisoft’s critically acclaimed Just Dance series. [7] The attackers targeted the IT infrastructure used by Ubisoft to run Just Dance. Player data compromised includes GamerTags, profile IDs, Device IDs, and some Just Dance videos. Ubisoft says an investigation has “not shown that any Ubisoft account information has been compromised as a result of this incident.” [7].

Serious games are effective in a healthcare environment due to the strong motivation and immersion that video games exert on their players, clinicians see them as interesting adjuncts to conventional physical rehabilitation in patients suffering from injury or disability. [6] To achieve its purpose, that serious game would need to collect data about the participant to not only analyse the effectiveness of the treatment and but also to evaluate the current status of the patient. The data these types of games would need to collect would differ and supersede the amount a regular game designed for entertainment would typically collect. Information collected about the participant – aside from the personal data already collected in a video game context - could be reflective of their medical history, lifestyle, and diet.

The data collected therefore by these games suddenly becomes interesting to a much wider number of interested parties. [4] This data collection needs to be agreed with patient and clearly explained what and how the data will be used. The data collected in serious games can influence a lot more than data collected by entertainment games.

Successful and effective game design obscures the player from information they do not need to complete the task. In entertainment games, this isn’t a problem as introduction levels are a common solution used to “train” the player for later portions of the game. When designing a serious game for

physical therapy for example, the gameplay has an obscured purpose which is to track the progress of patients and measure how physically capable they are/are becoming. Given this obfuscation from the end user is it even possible for the end user to give 'informed consent' in the way it was outlined earlier. [4]

January 2022

[1] Drachen, A., Seif El-Nasr, M., Canossa, A.,(2013) Game Analytics – The Basics, Game Analytics, Springer, London, 2013, pp. 13–40. DOI: 10.1007/ 978-1-4471-4769-5_2.

[2] Just Dance 2022.,(2021). PlayStation 4, Xbox One, Nintendo Switch, PlayStation 5, Xbox Series X and Series S, Google Stadia. Ubisoft.

[3] Kröger, J., Raschke, P., Campbell, J, P., Ullrich, S. (2021, July). Surveilling the Gamers: Privacy Impacts of the Video Game Industry. DOI:10.2139/ssrn.3881279

[4] McCall, R., Baillie, L. (2017, August). Ethics, Privacy and Trust in Serious Games. Handbook of Digital Games and Entertainment Technologies (2017), pp. 611 - 640. DOI: 10.1007/978-981-4560-50-4_37

[5] Russell, N., J Reidenberg, J., Moon, S., (2020) Privacy in Gaming, Fordham Intellectual Property, Media & Entertainment Law Journal (2020). DOI: [10.2139/ssrn.3147068](https://doi.org/10.2139/ssrn.3147068).

[6] Schijven, M,P., (2018, January). How Serious Games Will Improve Healthcare. Digital Health (pp.139-157). DOI: 10.1007/978-3-319-61446-5_10

[7] Slater-Robbins, M. (2021, December). Ubisoft says Just Dance was hit by a data breach. TechRader. Online: <https://www.techradar.com/news/ubisoft-says-just-dance-was-hit-by-a-data-breach>