Privacy in Gaming and Virtual Reality Technologies: Review of Academic Literature 2012 – 2017

July 13, 2017

Study Author

Sumyung Moon
Project Fellow, Fordham CLIP

CLIP Center on Law and Information Policy
AT FORDHAM LAW SCHOOL

Study Advisors

Joel R. Reidenberg
Academic Study Director, Fordham CLIP

N. Cameron Russell
Executive Director, Fordham CLIP

A grant from the Digital Trust Foundation to the Center on Law and Information Policy at the Fordham University School of Law, New York, NY (Fordham CLIP) supported work on this study.

The views and opinions expressed in this report are those of the authors and are not presented as those of any of the sponsoring organizations or financial supporters of those organizations. Any errors and omissions are the responsibility of the author.

Table of Contents

I. Analysis of the Academic Literature

Fordham CLIP initially identified 18 articles discussing data collection practices of gaming industry or virtual reality/augmented reality technology.[1] The dates of publications ranged from 2012 to 2017.[2] Once all citations were identified, Fordham CLIP reviewed the texts to identify themes and trends in scholarship.

These articles discuss either data practices of gaming platforms in general or privacy issues raised by development of virtual reality or augmented reality technology, with some overlap between the subjects. Although some of the articles focus exclusively on the discussion of one particular gaming platform - either mobile or traditional console - the majority of the articles address implications of data practices in privacy law in whole or in part. There has been a series of privacy debates in recent years about the data practices of traditional gaming platforms such as PC or console in light of the development of gaming devices. New technology has enabled game developers to capture player data not available before, and discussion of such data collection in VR/AR gaming platforms was often introduced as small part of a discussion of VR/AR technology generally.

[1] *See infra* Bibliography.

[2] Two articles were published in 2012. *See* Joshua A.T. Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, 27 Berkeley Tech. L. J. 55 (2012); Joshua A.T. Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, 2 U.C. Irvine L. Rev. 695 (2012). Three articles were published in 2014. *See* Joe Newman, *"Press Start to Track?" Privacy and the New Questions Posed by Modern Video Game Technology*, 42 AIPLA Q. J. 527 (2014); Matthew Ruskin, *Playing in the Dark: How Online Games Provide Shelter for Criminal Organizations in the Surveillance Age*, 31 Ariz. J. Int'l & Comp. L. 875 (2014); Yana Welinder, *Facing Real-Time Identification in Mobile Apps & Wearable Computers*, 30 Santa Clara High Tech. L. J. 89 (2014). Four articles were published in 2015. *See* Alexandra McDonald et al., *Mobile Apps: Redefining the Virtual California Economy and the Laws That Govern It*, 24 Competition: J. Antitrust, Unfair Competition L. & Privacy Sec. St. B. Cal. 86 (2015); Matthew Knopf, *Privacy Expectations in Online Video Games: In Light of Edward Snowden's NSA Document Leak*, 31 Syracuse J. Sci. & Tech. L. Rep. 98 (2015); Irina D. Manta & David S. Olson, *Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly*, 67 Ala. L. Rev. 135 (2015); Andreas Kotsios, *Privacy in an Augmented Reality*, 23 Int. J. L. & Info. Tech. 157 (2015). Five articles were published in 2016. *See* Jennifer Agate, *Gaming and Young People – The Right Concerns?*, 27 Ent. L. Rev. 13 (2016); Valeriel Verdoodt, *Toying with Children's Emotions, the New Game in Town? The Legality of Advergames in the EU*, 32 Computer L. & Security Rev. 599 (2016); Gilad Yadin, *Virtual Reality Intrusion*, 53 Willamette L. Rev. 63 (2016); David E. Fink & Jamie N. Zagoria, *VR/AR in a Real World*, 33 Ent. & Sports Law. 1 (2016); Roya Bagheri, *Virtual Reality: The Real Life Consequences*, 17 U.C. Davis Bus. L. J. 101 (2016). Four articles were identified for 2017, but one of them is not yet published. *See* Adrian Fong, *The Role of App Intermediaries in Protecting Data Privacy*, 25 Int. J. L. & Info. Tech. 85 (2017); Crystal Nwaneri, *Ready Lawyer One: Legal Issues in the Innovation of Virtual Reality*, 30 Harv. J. L. & Tech. 601 (2017); Alexander Schnider, *Virtual Reality: From your Home to Everywhere*, 39 Eur. Intell. Prop. Rev. 3 (2017); Mark A. Lemley & Eugene Volokh, Law, *Virtual Reality, and Augmented Reality* (Stanford Pub. L. Working Paper, No. 2933867 & UCLA School of Law, Public Law Research Paper No. 17-13, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933867.

A. Applicable Law Relevant to the Data Practices of Gaming Industry

Most articles examine existing legal frameworks that are applicable to several privacy issues in gaming.[3] One category of articles discusses specific statutes or regulation of particular subjects[4] and the other set of articles discusses whether expectation of privacy can exist in the data collected through gaming platforms.[5] In addition to analysis of the legal framework within the United States, the majority of articles also provide an analysis of available legal protections within European countries.[6]

1. Statutes and Regulations

Fordham CLIP identified a number of articles that examine how particular statutes could be applied to the practices of the gaming industry.[7] The focus of this type of literature varied from discussion of consumer protection law,[8] surveillance law,[9] children's privacy protection law,[10] and gaming platform liability[11] to application of state statutes.[12]

---

[3] *See* Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Knopf, *supra* note 2;Bagheri, supra note 2; Kotsios, *supra* note 2; Lemley *supra* note 2; Welinder, *supra* note 2; Fong, *supra* note 2; Schnider, *supra* note 2.

[4] *See* Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Mixed Reality: How The Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Knopf, *supra* note 2; Bagheri, *supra* note 2; Kotsios, *supra* note 2; Welinder, *supra* note 2; Fong, *supra* note 2.

[5] *See* Ruskin, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Knopf, *supra* note 2; Bagheri, *supra* note 2; Kotsios, *supra* note 2.

[6] *See* Schnider, *supra* note 2; Kotsios, *supra* note 2; Ruskin, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Bagheri, *supra* note 2; Welinder, *supra*; Fong, *supra* note 2.

[7] *See* Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Knopf, supra note 2; Bagheri, *supra* note 2; Kotsios, *supra* note 2; Welinder, *supra* note 2; Fong, *supra* note 2.

[8] *See* Welinder, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; McDonald et al., *supra* note 2; Newman, *supra* note 2; Kotsios, *supra* note 2.

[9] *See* Welinder, *supra* note 2; Bagheri, *supra* note 2; Knopf, *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Ruskin, *supra* note 2 (2014).

[10] *See* Newman, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Bagheri, *supra* note 2; Welinder, *supra* note 2.

[11] *See* Fong, *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Newman, *supra* note 2.

[12] *See* Newman, *supra* note 2; McDonald et al., *supra* note 2; Kotsios, *supra* note 2; Fong, *supra* note 2.

i. Consumer Protection

In this category of articles, authors examine existing consumer protection laws that can be applied to protect gamers from misinformation.[13] Some articles specifically discuss the Fair Credit Reporting Act ("FCRA") and its application to use of video game data.[14] If players' personal profiles or data is shared with insurers or employers and used to make credit, insurance, employment or housing determinations, game developers could be "consumer reporting agencies" as defined by 15 U.S.C. § 1681(b).[15] Thus, one author argues that under FCRA, game developers must take reasonable steps to ensure recipients of their player data have a "permissible purpose" for use of that information, developers take reasonable steps to ensure the highest possible accuracy of the information being collected, and game developers provide data recipients with information about their obligations under the law.[16] For example, apps which "score" users based on their economic proclivities could implicate FCRA.[17] Thus, under FCRA, the Federal Trade Commission (FTC) can also bring enforcement actions against third parties such as credit reporting agencies, data brokers, and companies furnishing information.[18]

Another topic frequently discussed by various articles was Section 5 of the FTC Act.[19] These articles argued that gaming platforms' data practices could violate the FTC's authority to police "unfair" or "deceptive" business practices under the Act,[20] which provides that "[u]nfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are hereby declared unlawful."[21] Thus, the FTC can bring enforcement actions against gaming and VR companies who transmit user's information to third parties in violation of what their privacy policies state.[22] The FTC has also used its enforcement authority to pursue companies that implemented ineffective data security measures or that deceived consumers by promising one thing in a privacy policy and then actually doing another thing with user data.[23]

One author observed that the FTC views consumer privacy as one of its top priorities, likely positioning the FTC as a key regulator for the video gaming industry.[24] However, some articles observed limits to the FTC's enforcement mechanisms.[25] One article argued that privacy enforcement by the FTC is unlikely because the scope of the FTC Act only extends to unfair or

---

[13] *See* Welinder, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; McDonald et al., *supra* note 2; Newman, *supra* note 2; Kotsios, *supra* note 2.
[14] *See* Newman, *supra* note 2, at 575-76; McDonald et al., *supra* note 2, at n.41.
[15] Newman, *supra* note 2, at 575.
[16] *Id.*
[17] *Id.* at 576.
[18] *See* McDonald et al., *supra* note 2, at n.41.
[19] *See* Welinder, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; McDonald et al., *supra* note 2; Newman, *supra* note 2; Kotsios, *supra* note 2.
[20] Newman, *supra* note 2, at 583.
[21] Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2, at 759.
[22] *Id.*
[23] Newman, *supra* note 2, at 584.
[24] *See id.*
[25] *See* Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2, at 759-760; Kotsios, *supra* note 2.

deceptive practice in or affecting commerce.[26] Also another limitation may arise from the End User License Agreements ("EULAs") between users and operators because the transmission of user data to authorized third parties is generally permitted under EULAs.[27] Thus, such transfers would not be considered as unfair or deceptive.[28] Another article argues that the FTC's role is limited in a sense that users cannot bring a private privacy action to the FTC to seek compensation for injuries that he or she has allegedly suffered.[29]

ii. Protection of Children's Privacy

A substantial number of articles address the law designed to protect children's privacy interests.[30] One article argued that children represent a large slice of the demographic of video game players, and several laws work to protect the privacy of children, both generally and in the educational context.[31]

The most cited statute from the identified literature was the Children's Online Privacy and Protection Act ("COPPA").[32] COPPA generally requires all online services or mobile applications collecting and sharing information about children under thirteen to obtain the child's parental consent, and to follow a number of other data-handling requirements.[33] Articles that reference COPPA argue that online game operators can fall within the scope of COPPA if they collect personal information for commercial purposes such as in-game or online targeted advertising.[34] Under COPPA's definition, "personal information" can be a child's name, address, phone number or email address, as well as any photos, videos, and audio recordings of the child and any persistent identifier such as IP address.[35] To avoid liability, game developers must take certain measures such as explicitly stating in the privacy policy that the game is not intended for use by anyone under age 13, requiring users to certify that they are over age 13 and enter their birthday, or requiring users to connect to the game via Facebook Connect, as Facebook requires its users be at least 13 years old.[36]

One article argued that COPPA has led to an increase in the use of age-gates and age verification systems on mobile games.[37] However, the author pointed out that appropriate

[26] Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2, at 759.
[27] See *id.*
[28] See *id.* at 759-760.
[29] Kotsios, *supra* note 2.
[30] *See* Newman, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Bagheri, *supra* note 2; Welinder, *supra* note 2.
[31] Newman, *supra* note 2, at 573.
[32] *See* Newman, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Knopf, *supra* note 2; Bagheri, *supra* note 2; Welinder, *supra* note 2.
[33] Newman, *supra* note 2, at 573.
[34] *See id.*; 573; McDonald et al., *supra* note 2; Agate, *supra* note 2; Bagheri, *supra* note 2.
[35] Newman, *supra* note 2, 573.
[36] McDonald et al., *supra* note 2.
[37] *See* Newman, *supra* note 2, at 574.

control of a gaming platform's data collection could be technically challenging.[38] The author gives an example of Xbox One Kinect, which is a console device that can collect information about every gamer in the room.[39] Where a child invites a friend over to play a game, Kinect's ability to collect information about that friend separately could be problematic when there is consent for one child and not for another.[40] In addition, Xbox One's Kinect offered a camera feature that had to be connected and always on to function properly.[41] One article argued that such feature would have violated COPPA and triggered public concern about the camera's surveillance capabilities and questions about how the data would be stored and used.[42]

In addition to COPPA, one article argued that children's privacy issues extend to how data is shared within the context of education.[43] For example, for game developers to collaborate with schools, educational institutions may require their compliance with the Family Educational Rights and Privacy Act of 1974 ("FERPA"), which addresses concerns about unauthorized, inappropriate releases of education records to individuals and organizations outside of the school environment.[44] The article noted that video games are increasingly used in the classroom and game developers and game developers should be aware of increasing concerns about the collection and use of data in education.[45]

iii. Surveillance

A number of articles addressed how third party uses of player data in gaming can violate several surveillance related laws.[46] In 2013, National Security Agency documents were leaked and those documents revealed that surveillance agencies of the United States and United Kingdom were conducting intelligence operations inside massive multiplayer online video games such as World of Warcraft.[47] One article argued that government agents could have created their own profiles and avatars in these games to collect or access the data or communications of players.[48] These articles identified that the Electronic Communications Privacy Act and Foreign Intelligence Surveillance Act could be relevant to such situations. The Electronic Communications Privacy Act ("ECPA") and its Wiretap Act and Stored Communication Act ("SCA") may require game developers to comply with government requests for user data.[49] Also, gaming platforms could be subject to government surveillance through the Foreign Intelligence Surveillance Act ("FISA"), which gives procedures to the government to conduct

[38] *Id.*
[39] *Id.* at 574 n.249.
[40] *See* Newman, *supra* note 2, at 574 n.249.
[41] *See* Bagheri, *supra* note 2, at 110-11.
[42] *See id.*
[43] Newman, *supra* note 2, at 574-75.
[44] *Id.*
[45] *Id.*
[46] *See* Welinder, *supra* note 2; Bagheri, *supra* note 2; Knopf, *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Ruskin, *supra* note 2.
[47] Knopf, *supra* note 2, at 99.
[48] *See id.*
[49] *See id.* at 112; Welinder, *supra* note 2.

physical and electronic surveillance of "foreign intelligence information" between "foreign powers" and "agents of foreign powers."[50] One article argues that while conducting surveillance on foreign targets, the government can "incidentally" obtain data on United States citizens and these fears over "incidental" collection of data is aggravated when taking into account the amount of personal and private data that can be collected thorough private computers and video game consoles during gaming.[51]

iv. State Laws

Some articles argue that state law can impose certain requirements for the protection of user privacy.[52] States such as Connecticut, Pennsylvania, Nebraska, and California impose their own enforcement mechanisms under state statute regarding privacy policy requirements.[53] For example, some articles referenced the California Online Privacy Protection Act ("CalOPPA") as the most extensive disclosure law.[54] CalOPPA requires that any entity collecting information from California residents inform consumers about their specific online data practices, including how they respond to browser "Do Not Track" signals.[55] One author referenced the California Attorney General guidelines regarding compliance with CalOPPA.[56] The guideline states that companies should disclose types of information collected from users, how information is used, how information is disclosed or shared with third parties, and how users can update or remove personal information, and impose notice requirement regarding how users will be informed when the privacy policy changes.[57] One author argues that sharing with third parties for profit-seeking purposes is particularly under scrutiny and that disclosure of anonymized and aggregated data for analytics purposes without user consent can result in litigation.[58]

In addition, one article referenced the Illinois Biometric Information Privacy Act which addresses the collection, use, safeguarding, handling, storage retention and destruction of biometric identifiers and applies to private entities.[59] The author further noted that there is no current federal legislative framework that addresses collection of biometrics.[60]

[50] Knopf, *supra* note 2 at 112.
[51] *See id.*
[52] *See* Newman, *supra* note 2; McDonald et al., *supra* note 2; Kotsios, *supra* note 2; Fong, *supra* note 2.
[53] McDonald et al., *supra* note 2, n.98-101.
[54] *See* Newman, *supra* note 2, at 584; McDonald et al., *supra* note 2.
[55] Newman, *supra* note 2, at 585.
[56] *See* McDonald et al., *supra* note 2.
[57] McDonald et al., *supra* note 2.
[58] *See id.*
[59] See Kotsios, *supra* note 2.
[60] See Kotsios, *supra* note 2.

2. Expectation of Privacy in Virtual Worlds

Another category of articles analyze the current legal framework with a focus on expectations of privacy in gaming platforms.[61] One article argued that, in general, personal identifiable information (PII) such as personal characteristics of the user including culture, age, religion, employment, credit history, and personal contact information receives much more privacy protection than non-PII.[62] The author however notes that because the virtual reality technology is so new, it is unclear whether there is an expectation of privacy for non-PII activities.[63]

Other articles argue that anonymity within online games could indicate an expectation of privacy for many gamers.[64] Users can often hide behind avatars and usernames, and because they do not personally know the parties with whom they communicate, online activity appears more anonymous.[65] One article focused on the difference between communication through social media and video games.[66] The author stated that one of the most important factors of video games is the ability to "virtually" become a different person and most gamers play within their own homes and on their own video game consoles.[67] Thus, privacy expectations of the gamer when they create an avatar in an online video game could be greater.[68] However, the author further noted that unlike traditional video game consoles which sole purpose was to play games, the current state of technology allows new type of consoles to emerge, and the ability to connect cellphone apps and social media has affected gaming and could hinder video game players' expectations of privacy.[69]

3. Industry Standards and Guidelines

Other types of articles introduce industry standards or guidelines in the gaming industry to respond to the scarcity of controlling case law.[70] These articles argue that private parties are undertaking efforts to preserve and redefine privacy by imposing either formal requirements or informal guidelines for developers that collect personal information.[71] For example, one article argued that the major console manufacturers generally require a list of all possible information exchanged between players and the software developer in order to approve a game for play on

---

[61] *See* Ruskin, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Knopf, *supra* note 2; Bagheri, *supra* note 2; Kotsios, *supra* note 2.
[62] *See* Bagheri, *supra* note 2 at 109.
[63] *See id.*
[64] *See* Ruskin, *supra* note 2; Knopf, *supra* note 2.
[65] Ruskin, *supra* note 2 at 890.
[66] Knopf, *supra* note 2, at 117-18.
[67] *See id.*
[68] *Id.*
[69] *See id.*
[70] *See* Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Kotsios, *supra* note 2; Nwaneri, *supra* note 2; Welinder, *supra* note 2; Fong, *supra* note 2.
[71] *See* McDonald et al., *supra* note 2.

their machine.[72] Similarly, companies like Apple and Google require app developers to follow their data programs as a condition of selling games on their respective app stores.[73]

Additionally, the Entertainment Software Rating Board ("ESRB")'s "Privacy Certified" program assesses privacy risks and ensures that game companies are compliant with most privacy laws and regulatory frameworks.[74] Another example is the Digital Analytics Association's web analyst code of ethics that incorporates principles of privacy, transparency, consumer control, education, and accountability into the conduct of analytics.[75]

B. Data Practices of Gaming Platforms and Their Interaction with Gamers

Fordham CLIP identified its list of academic literature based on whether the article includes a substantial amount of discussion regarding data practices of gaming platforms. Thus, a discussion of data practices in relation to video games or virtual reality/augmented reality technology appeared in almost every article.[76]

1. Data Collection

In summary, data can be categorized as either aggregated data of a large population of players or individualized data of each player.[77] Game developers use aggregated data in order to predict new trends and patterns throughout large sections of its player base, but the collection of individual data is most under the scrutiny.[78] Modern video games increasingly collect player data from outside the game environment through a variety of sensors and other sources.[79]

A majority of articles shared similar ideas regarding the types of data that could be collected by uses of gaming platforms. First, many articles noted that data about specifics of a gamer's device such as smartphone, PC, or console models could be collected by the developer.[80] Also, tracking technologies such as cookies and beacons can be used or even browsing history could be collected.[81] Second, players' personally identifiable information such

---

[72] *See* Newman, *supra* note 2, at 586-87.
[73] *Id.*
[74] *Id.*
[75] *Id.*
[76] *See* Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Mixed Reality: How The Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Knopf, *supra* note 2; Manta & Olson, *supra* note 2; Bagheri, *supra* note 2; Kotsios, *supra* note 2; Lemley & Volokh, *supra* note 2; Nwaneri, *supra* note 2; Welinder, *supra* note 2; Fink & Zagoria, *supra* note 2.
[77] *See* Newman, *supra* note 2, at 545.
[78] *Id.*
[79] *Id.*
[80] *See* McDonald et al., *supra* note 2.
[81] Fong, *supra* note 2; Verdoodt, *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2.

age, name, and e-mail address is commonly collected through gaming.[82] Lastly, almost every article noted that collection of geolocation data is common practice,[83] especially in the context of AR gaming platforms.[84]

Some articles discussed data practices with more specific focus. These articles argue that depending on what types of apps or gaming software players are using, sensitive information such player's face or voice can be collected.[85] Console platform games frequently feature integrated cameras and developers use captured images to enhance immersion in their game worlds.[86] For example, such data can be captured when a player creates an avatar using his or her real-world image.[87] In addition, player's facial information can be captured in other ways when the company uses facial data to identify and sign in players as a security measure.[88] Also, many gaming platforms increasingly capture player's voice.[89] For example, that data is captured when gamers create a voice profile within a gaming platform.[90]

Some articles highlighted data collection of social features such as chat logs between players or contacts list.[91] One article referenced Microsoft's policy which warned players that they should not expect any level of privacy concerning the use of the live communication features such as voice chat, video and communications.[92] However, one article argues that gamers could have an expectation of privacy in those communications within gaming platforms because social features such as chat or messaging is often restricted to a guild, party, or group of friends.[93] In addition, most modern gaming platforms allow players to contact and "friend" each

---

[82] Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Verdoodt, *supra* note 2; Knopf, *supra* note 2; Manta & Olson, *supra* note 2; Bagheri, *supra* note 2; Kotsios, *supra* note 2; Lemley & Volokh, *supra* note 2; Nwaneri, *supra* note 2; Welinder, *supra* note 2; Fong, *supra* note 2; Schnider, *supra* note 2; Fink & Zagoria, *supra* note 2; Yadin, *supra* note 2.
[83] *See* Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Verdoodt, *supra* note 2; Knopf, *supra* note 2; Manta & Olson, *supra* note 2; Bagheri, *supra* note 2; Kotsios, *supra* note 2; Lemley & Volokh, *supra* note 2; Nwaneri, *supra* note 2; Welinder, *supra* note 2; Fong, *supra* note 2; Schnider, *supra* note 2; Fink & Zagoria, *supra* note 2; Yadin, *supra* note 2.
[84] *See* Kotsios, *supra* note 2.
[85] Kotsios, *supra* note 2; Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Knopf, *supra* note 2; Bagheri, *supra* note 2; Lemley & Volokh, *supra* note 2; Welinder, *supra* note 2; Yadin, *supra* note 2.
[86] Newman, supra note 2, at 553.
[87] *Id.*
[88] *Id.* at 552.
[89] *Id.*
[90] *Id.*
[91] *See* Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, Avatar Experimentation: Human Subjects Research in Virtual Worlds, *supra* note 2; Knopf, *supra* note 2; Lemley & Volokh, *supra* note 2; Yadin, *supra* note 2.
[92] *See* Newman, *supra* note 2, at 553.
[93] *See* Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2, at 775.

other.[94] In fact, in the mobile game platforms, a sub-genre of "social games" has emerged such as Facebook's new forms of gameplay which allow players to interact with friends.[95]

Articles are also focusing on development of new technologies by discussing collection of players' biometrics such as heart rate, weight, skin response, brain activity, eye-tracking, physical movement and dimensions.[96] One article referenced the example of console platforms such as Wii Fit or Microsoft's Kinect fitness games.[97] These types of health training games can use a player's weight and movement data in order to chart a player's physical health over time or adjust the in-game difficulty based on data received from the player's heart rate.[98]

A majority of articles also explore particularly controversial uses of data in modern games and VR/AR technologies involving the use of players' detailed psychographic profile or cognitive skills.[99] One article argues that every single player behavior can be tracked and manipulated, dramatically expanding the scope of potential privacy concerns.[100] Such collection could be through games that monitor a player's in-game decisions and personality profile.[101] Also, a growing number of games can track a player's cognitive skills, such as memory, attention, speed, flexibility, and problem solving ability.[102] For example, one article explored the mobile platform game Candy Crush Saga, arguing that developers will monitor player performance and make game levels easier if too many players get stuck.[103] In addition to use of a player's psychographic profile to adjust difficulty in gaming, a player's economic proclivities could be predicted by collecting data about how players spend real-world money for in-game purchases.[104]

2. Data Usage

In addition to discussion of data collection, a majority of articles further examine how collected data is used by gaming platform developers or how it is shared with third parties.[105]

---

[94] Newman, *supra* note 2, at 555.
[95] *Id.*
[96] *See* Kotsios, *supra* note 2; Newman, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Manta & Olson, *supra* note 2; Lemley & Volokh, *supra* note 2; Nwaneri, *supra* note 2; Welinder, *supra* note 2; Fong, *supra* note 2; Schnider, *supra* note 2; Fink & Zagoria, *supra* note 2.
[97] Newman, *supra* note 2, at 536-38.
[98] *Id.*
[99] *See* Yadin *supra* note 2; Newman, *supra* note 2; Ruskin, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Verdoodt, *supra* note 2; Knopf, *supra* note 2; Manta & Olson, *supra* note 2; Bagheri, *supra* note 2; Kotsios, *supra* note 2; Lemley & Volokh, *supra* note 2; Nwaneri, *supra* note 2; Schnider, *supra* note 2; Fink & Zagoria, *supra* note 2.
[100] *See* Bagheri, supra note 2.
[101] Newman, *supra* note 2, at 542.
[102] *Id.* at 558.
[103] *Id.* at 560-561.
[104] *Id.*
[105] *See* Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Knopf, *supra* note 2; Manta

i. Game Developers

Game developers analyze player information to enhance gaming experience by assuring the quality of the game.[106] For example, when developers discover that some game features are not functioning as intended, developers can transmit updates to the game to fix the problem.[107] In addition, developers also use player data to develop new, innovative in-game features, drive monetization of in-game purchases, and better regulate "virtual" economies within games.[108] One article argued that, in general, such use of aggregated player data raises fewer privacy concerns because of the difficulty in tying data to any individual.[109]

However, developers also collect individual data of player.[110] For example, individual player data is used by developers to identify players who are engaged in fraudulent activity within gaming such as identifying players who have modified the game or who are using cheating devices.[111]

Many articles argue that larger developers frequently analyze players' biometric data to test the game environment.[112] Biometric data could be retained when the player displays a strong emotional or physical reaction to the game during gameplay.[113] Also, eye-tracking information can be retained when players shows a strong interest in the particular gaming interface.[114] One article explored how game developers incorporate biometric data such as heart rate and how this can be used to adjust in-game difficulty depending on a player's reaction.[115]

Lastly, collection of location data by developers were frequently analyzed by the academic articles focused on augmented reality technologies.[116] Geolocation data can be used to compare a player's performance to other players in the same geographic area.[117]

& Olson, *supra* note 2; Bagheri, *supra* note 2; Kotsios, *supra* note 2; Lemley & Volokh, *supra* note 2; Nwaneri, *supra* note 2; Welinder, *supra* note 2; Fink & Zagoria, *supra* note 2.

[106] Newman, *supra* note 2, at 544-47.

[107] *Id.*

[108] *Id.*

[109] *See* id. at 547.

[110] *Id.*

[111] *Id.*

[112] *See* Kotsios, *supra* note 2; Newman, *supra* note 2; McDonald et al., *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2; Manta & Olson, *supra* note 2; Lemley & Volokh, *supra* note 2; Nwaneri, *supra* note 2; Welinder, *supra* note 2; Fong, *supra* note 2; Schnider, *supra* note 2; Fink & Zagoria, supra note 2.

[113] Newman, *supra* note 2, at 549.

[114] *Id.*

[115] *See id.* at 550.

[116] *See* Kotsios, *supra* note 2.

[117] Newman, *supra* note 2, at 551.

ii. Third Parties

Some articles point out that that use of player data will not be confined to the game environment.[118] These articles describe situations where player data is commonly used outside of the game and shared with third parties.[119]

One example of how data is shared with third parties is the online statistics reporting system across gaming platforms.[120] One article reported that gaming platforms track a player's performance across games and onto other platforms such as Steam, PlayStation Network, or iOS Game Center.[121] Then, information is shared again with third party aggregators who visualize a player's achievements from multiple platforms into a single player dossier.[122] The author further argues that this data practice can lead to problems because players can track not only their performances but also those of their friends across other gaming platforms.[123]

Many articles also argue that developers share player data with third parties for targeted advertising purpose.[124] These articles argue that a player's personal profile is used to increase manipulative effects of targeted advertising by applying analytics appealing to that player's emotion.[125] For example, a player's purchasing habits within a gaming platform can be shared with third parties for marketing purposes.[126] Many platforms offer a virtual market where a player can buy games and other digital content and a player's real world attributes or in-game behavior can be collected and shared for predictive marketing purposes.[127] The author argues that, however, retention of such information by developers or third parties is dangerous because they can exploit a player's psychological vulnerabilities towards certain products to discriminate against the player.[128] One article gives an example of how a player's physical location information is used in advertising.[129] On Xbox 360 and Xbox One, an integrated Pizza Hut app obtains and uses a player's physical location to send offers for local pizza delivery that can be placed through the gaming console.[130]

User personal information can be shared in unexpected situations as well.[131] Several articles show how the video game industry is particularly vulnerable to data leaks and security

---

[118] Fink & Zagoria, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Knopf, *supra* note 2. Newman, *supra* note 2.
[119] Fink & Zagoria, *supra* note 2; Agate, *supra* note 2; Verdoodt, *supra* note 2; Knopf, *supra* note 2. Newman, *supra* note 2.
[120] Newman, *supra* note 2, at 564.
[121] *See id.*
[122] *Id.*
[123] *See id.* at 565.
[124] *See* Agate, *supra* note 2; McDonald et al., *supra* note 2; Verdoodt, *supra* note 2; Newman, *supra* note 2; Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, *supra* note 2.
[125] *See* Verdoodt, *supra* note 2; Newman, *supra* note 2, at 565-66.
[126] Fong, *supra* note 2.
[127] Newman, *supra* note 2, at 566.
[128] *See id.*
[129] *See id.*
[130] Newman, *supra* note 2, at 566.
[131] *Id.* at 571.

breaches by hackers.[132] In addition, government may have an interest in player data as a tool used against a player in legal matters.[133] For example, one article referenced "Operation Game Over," which was a government program to remove all sex offenders from online platforms.[134]

C. Negative Implications

Several articles described specific data breach incidents to demonstrate harms caused by invasive data collection practices of gaming platforms.[135] The most cited incident of data breach is the hacking of PlayStation Network in 2011, which was often illustrated as the largest data breach in gaming platform.[136] Sensitive personal data and credit card information of over 77 million users were compromised as a result of the hack in addition to $171 million that it cost Sony.[137] One article noted that despite the seriousness of the breach, Sony did not make any further repercussions or changes in privacy protections.[138]

In addition to hams caused by data breaches, some articles argue that invasive consumer data collection could result in price discrimination,[139] disclosure, and mass surveillance.[140] For example, a player's psychological vulnerabilities can be exploited by sellers to manipulate prices of games to discriminate against the player or offer products specifically targeted for vulnerable gamers.[141] Furthermore, in the video game environment, even though the average player may not be aware of privacy issues, they might be concerned if gaming habits were used to reveal sexual history, misconduct, or physical well-being.[142]

D. Recommendations

A majority of articles provided recommendations or proposed solutions to regulate data collection practices of gaming platforms or VR/AR technologies. One category of articles calls for legislative actions,[143] and others argue that gaming platforms should self-regulate.[144] Other

---

[132] *See* Newman, *supra* note 2; McDonald et al., *supra* note 2; Knopf, *supra* note 2; Bagheri, *supra* note 2; Nwaneri, *supra* note 2; Welinder, *supra* note 2; Yadin, *supra* note 2.
[133] Newman, *supra* note 2, at 571.
[134] *See* Knopf, *supra* note 2, at 128-29.
[135] *See* Newman, *supra* note 2; McDonald et al., *supra* note 2; Knopf, *supra* note 2; Bagheri, *supra* note 2; Nwaneri, *supra* note 2; Welinder, *supra* note 2; Yadin, *supra* note 2.
[136] *See* Knopf, *supra* note 2, at 128.
[137] *Id.*
[138] *See* Bagheri, *supra* note 2, at 110.
[139] *See* Newman, *supra* note 2; Manta & Olson, *supra* note 2; Nwaneri, *supra* note 2.
[140] *See* Welinder, *supra* note 2; Bagheri, *supra* note 2; Knopf, *supra* note 2; Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Ruskin, *supra* note 2.
[141] Newman, *supra* note 2, at 567.
[142] *Id.* at 590-91.
[143] *See* Kotsios, *supra* note 2; Verdoodt, *supra* note 2; Nwaneri, *supra* note 2; Bagheri, *supra* note 2; Welinder, *supra* note 2; Fong, *supra* note 2; Schnider, *supra* note 2.
[144] *See* Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fong, supra note 2.

articles argue that gamers and consumers of VR/AR technologies must be better informed about their privacy rights.[145]

Articles argue that the task of regulating data practices should be left to game creators themselves.[146] One article argues that game developers should focus on ensuring that their data practices are consistent with a gamer's expectation of privacy within the gaming platform.[147] Another article argues that because game developers are in the best position to monitor activities of gamers, developers can best implement security measures across their own networks.[148] This author further argues that developers' economic interests of retaining customers would encourage them to effectively respond to consumer privacy concerns.[149]

One article also notes that platform operators such as app intermediaries have an important role in ensuring protection of user data.[150] Unlike game developers, app stores, as intermediaries, do not themselves directly involve with data practices or control collected data.[151] However, the author argues that such intermediaries can help game developers by setting standards which ensure that game developers have privacy policies and practices when collecting personal data.[152]

Other articles call for more awareness from users regarding their privacy.[153] One article raises concern over a young generation who shares their personal data without sufficient awareness.[154] Another argues that consumers can contribute to the terms of contract, and privacy policies can be effective with opt-in options or certain defaults.[155]

Finally, a majority of articles call for legislative actions or government's involvement.[156] These types of articles argue that the need to create a legal, technological and social framework that will address these issues will be increasingly necessary.[157] One article argues that the privacy rights associated with virtual reality devices should be addressed as quickly as possible to protect consumer information because players cannot afford to wait to regulate privacy rights when companies are already collecting user information and damage is already occurring.[158] The

[145] *See* Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Agate, *supra* note 2.
[146] Newman, *supra* note 2; Ruskin, *supra* note 2; McDonald et al., *supra* note 2; Fong, *supra* note 2.
[147] Newman, *supra* note 2, at 991-92.
[148] Ruskin, *supra* note 2, at 907.
[149] *See* Ruskin, *supra* note 2, at 907.
[150] *See* Fong, *supra* note 2.
[151] Fong, *supra* note 2.
[152] *See* Fong, *supra* note 2.
[153] *See* Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2; Agate, *supra* note 2.
[154] *See* Agate, *supra* note 2, at 17.
[155] *See* Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, *supra* note 2, at 116.
[156] *See* Kotsios, *supra* note 2; Verdoodt, *supra* note 2; Nwaneri, *supra* note 2; Bagheri, *supra* note 2; Welinder, *supra* note 2; Fong, *supra* note 2; Schnider, *supra* note 2.
[157] *See* Kotsios, *supra* note 2.
[158] *See* Bagheri, *supra* note 2.

article further notes that reactive regulation would likely have only minimal effect if there would be no effective way to retrieve gamer's information that was already collected by platforms.[159]

[159] *See id.*

Bibliography

2012

1. Joshua A.T. Fairfield, *Mixed Reality: How the Laws of Virtual Worlds Govern Everyday Life*, 27 Berkeley Tech. L. J. 55 (2012).
2. Joshua A.T. Fairfield, *Avatar Experimentation: Human Subjects Research in Virtual Worlds*, 2 U.C. Irvine L. Rev. 695 (2012).

2014

3. Joe Newman, *"Press Start to Track?" Privacy and the New Questions Posed by Modern Video Game Technology*, 42 AIPLA Q. J. 527 (2014).
4. Matthew Ruskin, *Playing in the Dark: How Online Games Provide Shelter for Criminal Organizations in the Surveillance Age*, 31 Ariz. J. Int'l & Comp. L. 875 (2014).
5. Yana Welinder, *Facing Real-Time Identification in Mobile Apps & Wearable Computers*, 30 Santa Clara High Tech. L. J. 89 (2014).

2015

6. Alexandra McDonald et al., *Mobile Apps: Redefining the Virtual California Economy and the Laws That Govern It*, 24 Competition: J. Antitrust, Unfair Competition L. & Privacy Sec. St. B. Cal. 86 (2015).
7. Matthew Knopf, *Privacy Expectations in Online Video Games: In Light of Edward Snowden's NSA Document Leak*, 31 Syracuse J. Sci. & Tech. L. Rep. 98 (2015).
8. Irina D. Manta & David S. Olson, *Hello Barbie: First They Will Monitor You, Then They Will Discriminate Against You. Perfectly*, 67 Ala. L. Rev. 135 (2015).
9. Andreas Kotsios, *Privacy in an Augmented Reality*, 23 Int. J. L. & Info. Tech. 157 (2015).

2016

10. Jennifer Agate, *Gaming and Young People – The Right Concerns?*, 27 Ent. L. Rev. 13 (2016).
11. Valeriel Verdoodt, *Toying with Children's Emotions, the New Game in Town? The Legality of Advergames in the EU*, 32 Computer L. & Security Rev. 599 (2016).
12. Roya Bagheri, *Virtual Reality: The Real Life Consequences*, 17 U.C. Davis Bus. L. J. 101 (2016).
13. David E. Fink & Jamie N. Zagoria, *VR/AR in a Real World*, 33 Ent. & Sports Law. 1 (2016).
14. Gilad Yadin, *Virtual Reality Intrusion*, 53 Willamette L. Rev. 63 (2016).

2017

15. Mark A. Lemley & Eugene Volokh, *Law, Virtual Reality, and Augmented Reality* (Stanford Pub. L. Working Paper, No. 2933867 & UCLA School of Law, Public Law Research Paper No. 17-13, 2017), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2933867.

16. Crystal Nwaneri, *Ready Lawyer One: Legal Issues in the Innovation of Virtual Reality*, 30 Harv. J. L. & Tech. 601 (2017).
17. Adrian Fong, *The Role of App Intermediaries in Protecting Data Privacy*, 25 Int. J. L. & Info. Tech. 85 (2017).
18. Alexander Schnider, *Virtual Reality: From your Home to Everywhere*, 39 Eur. Intell. Prop. Rev. 3 (2017).