NEWS
UPDATE
International Journal of Advanced Mass Communication and Journalism

E-ISSN: 2708-4469
P-ISSN: 2708-4450
IJAMCJ 2022; 3(2): 38-47
© 2022 IJAMCJ
www.masscomjournal.com
Received: 17-04-2022
Accepted: 21-05-2022

Dr. Debastuti Dasgupta
Assistant Professor,
Department of Journalism and Mass Communication Asutosh College, Kolkata, West Bengal, India

Soumyadeep Sarkar
Student, University of Calcutta, Kolkata, West Bengal, India

Privacy: A myth in online gaming?

Dr. Debastuti Dasgupta and Soumyadeep Sarkar

DOI: https://doi.org/10.22271/27084450.2022.v3.i2a.49

Abstract

While online games have become an essential aspect of 21st-century entertainment, it must be remembered that this sometimes comes at the expense of one's privacy. It is well known that games capture and retain user data, which might be abused by other parties.

This exposes the video gaming business to hackers, who can exploit the exposed data to target individuals. This throws into question gaming businesses' ethical obligation to secure their consumers' privacy and data.

The researchers will investigate this by using case studies of the online battle royale game PUBG, Pokémon Go, and Angry Birds, as well as conducting interviews with gamers. It will discuss why gamers are vulnerable to hacking, the ethical and security considerations associated with sensitive data collecting, and what actions users may take to protect themselves and their privacy. It was discovered that in the gaming sector, ethics and user privacy must go together.

Keywords: Online gaming, privacy, PUBG mobile, pokémon go, angry birds

1. Introduction

This is the age of the internet, where nearly five billion people stay connected as they engage, communicate, and interact while disregarding geographical barriers. With its host of information and communication facilities, the internet has fostered the growth of an online environment that constitutes the actions and interactions of billions of beings across the globe. As people begin to interact and communicate with others in this online environment, individuals with similar interests and views congregate in groups. These groups are the stepping stone to the formation of virtual communities, where individuals transcend geographical and political barriers and pursue common goals and interests. In virtual communities, the members share a bond of commonality and connect through specific channels of media. This may include social media platforms such as Facebook, Instagram, and Twitter, or messaging social platforms such as Discord and WhatsApp.

The catch to this nigh-instantaneous connection with billions across the globe is the threat to the privacy of users. In a world where everything is connected, it is difficult to keep anything "private" as every individual connected to the internet are under constant surveillance (Mekovec, 2010) [18]. Not only does it render the individual vulnerable to companies that monitor their online activity, but it also leaves their personal data at risk.

And there lies the crux of the matter. Data is the "clay" with which companies build the "bricks" to offer what they call a better experience for users on the internet. One of the most common ways in which companies utilize user data is using them for targeted advertising (Ng, 2021) [29]. Targeted advertising serves a specific audience and is based on their demographics, interests, preferences, location, behaviours, and other factors (Natividad, 2020) [28]. Google, for one, is known to utilize this method with data harvested from its considerable user base.

Facebook, regarded as the king of social media, collects notorious amounts of user data – ranging from personal data such as their locations, names, and ages, to their preferences and online footprints. This goes directly to its data machine, and its algorithm determines what to show those users based on the same data.

It all comes back to the same – data. In an age of digital connections and virtual worlds, where people engage in activities ranging from business and managing their finances to staying connected, relaxing, or shopping, data is the central element that keeps things up and running.

Correspondence
Dr. Debastuti Dasgupta
Assistant Professor,
Department of Journalism and Mass Communication Asutosh College, Kolkata, West Bengal, India

This is partly why Clive Humby, renowned British mathematician and data science entrepreneur, called data the "new oil." Just like unrefined oil can be changed to make substances like plastic (Golson, 2021) [11], data can be "broken" down and analysed for it to have a variety of uses.

According to the Organisation for Economic Co-operation and Development (OECD), the ownership of data simultaneously rose with the rise in volumes of data, and the international bandwidth usage was increasingly shifting towards content providers such as Amazon, Google, Facebook, and Microsoft, among others (OECD, 2019) [30].

This harvesting and utilization of user data has also led to what would eventually be known as the digital economy. The umbrella term that comprises of all economic activities, professional interactions, and commercial transactions that occur on the internet using the World Wide Web (WWW), blockchain technologies, and ICT.

Based entirely on digital technologies, it has grown and evolved rapidly over the years alongside breakthroughs made in digital technology. The statistics speak for itself – the digital economy is equivalent to 15.5% of the total GDP of the world (N.A., Digital Development, 2022) [22, 23, 24, 25, 26, 27], and is slated to grow at an exponential rate over the years. For reference, the digital economy in India is expected to grow to reach $800 billion by 2030 (Digital economy to see exponential growth to $800 bn by 2030: FM, 2022).

With data being the driving force behind the digital economy, it must be ensured that it must not come at the cost of the privacy of users. Each and every action taken on the internet, no matter how small or insignificant, will remain in cyberspace. Nothing ever truly gets "deleted" from the internet no matter what actions are taken by the user, which includes clearing their browser history (Perkins, 2020) [33].

In the words of Jeffrey Rosen, "where every online photo, status update, Twitter post and blog entry by and about us can be stored forever." (Rosen, 2010) [35].

With users being unable to remove their digital footprints, the data, which is often personal by nature, remains vulnerable and exposed. This leads to a direct breach in the privacy of the users as companies and individuals recover the data for their own purposes. Even a mundane thing like a selfie, which one may take and post on a social media platform before taking it down, remains buried under other data and can be misused by anyone. This often leads to privacy concerns for the users, especially women (Dhir, Torshiem, Pallesen, & Andreassen, 2017) [8].

In the current study, the researcher has the following objectives:

1. To determine the threats to the privacy of users while gaming,
2. To determine whether the discovered ethical issues and norms of privacy in gaming reflect reality,
3. To determine what gamers, believe are the ethical responsibilities of companies to preserve their privacy.

1.1 What is privacy?

Privacy is something that is intangible, yet it is multidimensional and comprises a crucial part of one's life. The concept of privacy can be defined in several manners: "the state of being alone and not watched or interrupted by other people," by Oxford Learner's Dictionaries (2022). "The state of being free from unwanted or undue intrusion or disturbance in one's private life or affairs; freedom to be let alone," by Dictionary.com (2022). "The state of being alone, or the right to keep one's personal matters and relationships secret, by "Cambridge Dictionary (2022). "the quality or state of being apart from company or observation" by Merriam-Webster (2022).

All of the above definitions share a common element – privacy is the right of individuals to having some degree of control over how their personal information is harvested and used by others. Privacy is, undoubtedly, a human right, and Warren and Brandeis (1890) [46] underlines the same in the article "The Right to Privacy."

They argued that the right to privacy was the "right to be alone," asserting that the law afforded "a principle which may be invoked to protect the privacy of the individual from invasion either by the too enterprising press, the photographer, or the possessor of any other modern device for recording or reproducing scenes or sounds." (Warren & Brandeis, 1890) [46].

Britz (1996) [3] argues that privacy is the stepping stone to recognizing a person's freedom and personal autonomy.

1.2 Privacy in the age of the internet

Unsurprisingly, the same technology that has connected billions across the globe and achieved what many thought to be impossible, has turned out to be a major bane of privacy. "Privacy is one of the biggest problems in this new electronic age. At the heart of the Internet culture is a force that wants to find out everything about you. And once it has found out everything about you and two hundred million others, that's a very valuable asset, and people will be tempted to trade and do commerce with that asset. This wasn't the information that people were thinking of when they called this the information age," Andrew Grove, co-founder and former CEO, Intel Corporation, in an interview (Grove, 2007) [13]. Fifteen years down the line, the same holds true for users of the internet. With the coming of the internet came a horde of concerns as people, corporations, and governments were worried about protecting their privacy. Their concerns were further compounded by the fact that digital footprint can never truly be erased – that is, once something is on the internet, it will remain there even if it has been supposedly taken down. This has birthed a new concept – online privacy. Also known as digital or internet privacy, it refers to the level of protection that is given to the personal safety and security of an individual. "The complex issue of computer privacy covers the way your personal information is used, collected, shared, and stored on your personal devices and while on the Internet," according to Winston & Strawn LLP (Winston & Strawn, n.d.) [49].

Years after Warren and Brandeis' article, Westin (1967) [47] expanded their definition of privacy to include freedom from surveillance and the protection of one's personal autonomy. This concept of privacy later went on to include the ability of a person to personally control information about themselves (Stone, Gueutal, Gardner, & McClure, 1983) [43].

Mason (1986) [16] built on this, adding that it was one of the four ethical issues of the information age. He gave the ethical issues an acronym – PAPA (Privacy, Accuracy, Property, and Accessibility). According to Mason, there were two main forces that threaten the privacy of individuals-the rapid growth and proliferation of information technology (which culminated in the creation of the internet), and the increased value of information in decision-making.

What makes it so hard to maintain individual privacy on the internet is one’s digital footprint. This digital footprint includes the traces of every online activity of a user, ranging from shopping online and sharing emails to browsing websites, scrolling through social media feeds, and playing online games. While a strong online presence helps in fostering and maintaining connections across the globe, it makes it exceedingly difficult for the user to remove their digital footprint.

1.3 The offline consequences of the invasion of online privacy

With the widespread use of the internet, the personal information of data is constantly shared, both actively and passively, as users build on their online presence with activities such as browsing through websites. Cookies, for example, are designed to specifically track and record websites that are frequently visited by users. This information can be sold to companies to enable targeted ads for the user (Durnell, Okabe-Miyamoto, Howell, & Zizi, 2020) [9]. While targeted ads are a (relatively) harmless use of personal information, the same data obtained by websites and companies can be accessed or hacked in case of security breaches. This has been noticed in the cases of security breaches such as LinkedIn, which resulted in the personal data of around 700 million LinkedIn users being exposed and put up for sale (Morris, 2021) [20]. Other examples of customer data being exposed (and often put up for sale on the dark web) include Cleartrip (Singh, 2022) [39], Bizongo (Singh, 2021) [38], and Spotify (Stahie, 2020) [42].

It is thus evident that concerns about online privacy are warranted, and have gone up over the years. Wang, Genc, and Peng (2020) [45] inform that most of the research on online privacy and its concerns have revolved around that attitudes of users about how companies and other organizations store, use, collect, and sell their personal information.

The fruits borne of this extensive research include legal steps to safeguard the privacy of users on the internet, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR). The CCPA gives users the following basic rights to control their personal information on the internet:

1. The right to know what personal information is collected, used, and shared,
2. The right to be forgotten: The deletion of the personal information that was shared,
3. The right to opt out from sharing personal information, and
4. The right to non-discrimination for exercising of CCPA rights.

One of the biggest concerns of online privacy is the lack of general awareness of users. This refers not to the lack of awareness of the threats to online privacy, but rather to the fate of the personal information that is collected and used by companies.

A Pew Research report (Auxier, *et al*., 2019) [1] finds that a big chunk of American internet users believe that they have no control over their personal data collected by governments and private companies. They believe that their online and offline activities are being tracked constantly, and that the potential risks of collection of user data far outweighed the benefits. This creates a contradiction, since data-driven services are often touted to provide a better user experience and even save time and money.

In the same year, a report by Consumers International and the Internet Society (2019) [40] found that 69% of consumers were concerned about the collection of their personal data by mobile apps, while 63% found the harvesting of data by connected devices “creepy.”

This belief that individuals have no control over their personal data being collected in a variety of ways has led to an increase in privacy concerns. This rise in privacy concerns has even resulted in governments stepping in to put forth regulations for the collection of data, as is evident by the GDPR (Goswami, 2020) [12].

Buchanan *et al*. (2007) [4] used three short Internet-administrated scales in order to measure privacy-related attitudes – that is, concerns about digital privacy, the misuse of data, and online fraud – and behaviours – referring to general caution and technical protection availed by users. The facets covered by their research (which used the Measure of Online Privacy Concern and Protection for Use on the Internet) differed from the ones measured by Westin Privacy Segmentation Scale (Westin, 1998) [48].

Baruh and Cemalcilar’s scale (2014) [2], on the other hand, included four factors in its scale – privacy as a right, concerns about privacy regarding one’s personal information, concern about the privacy of other individuals, and other-contingent privacy.

Apart from identity theft, online fraud, theft of intellectual property, and the leaking of confidential information, what makes online privacy all the more important is that it often spills into the real world. Previous instances of the leak of personal information during data breaches leaves individuals and companies vulnerable and often does irreversible damage to their reputations.

This was highlighted in 2014, when private images of countless celebrities – mostly women – were leaked on the Internet for all to see after their iCloud accounts were hacked (McCormick, 2014) [17]. iPhone maker Apple later informed that tactics such as phishing and brute-force attack guessing were employed to invade the privacy of the celebrities and release their pictures on the Internet.

1.4 Ethics of online privacy

Derived from the ancient Greek word *ēthikós*, meaning "relating to one's character,” ethics have been defined in a variety of ways over the years. At its core, ethics refer to the moral principles that govern a person’s behaviour; the set of well-founded standards of right and wrong that prescribe what an individual ought to do. Several noteworthy individuals have laid down their definitions of ethics: “Ethics is the science of the ideal human character, the science of moral duty”, says Rushworth Kidder, founder of the Institute for Global Ethics (Kidder, 1995) [15]. “Ethics is a set of concepts and principles that guide us in determining what behavior helps or harms sentient creature, according to Richard William Paul and Linda Elder (Paul & Elder, 2006) [32] The 21st century is an age of informationalization, where data is the key to driving economic activities. Spinello (1995, p. 14) [41] insists that it is the very purpose of ethics to help individuals behave more honourably and attain those basic goods that make people more fully human.

Tene and Polonetsky (2012) [44] argue that the benefits of data collection are many, and in specific circumstances – such as law enforcement collecting data to tackle crimes and intelligence agencies uncovering terrorist plots – the collection of data is necessary. Nonetheless, it must be ensured that this does not come at the cost of the privacy of users and that a balance is reached. Eli M. Noam, professor of Finance and Economics at the Columbia Business School and the director of the Columbia Institute for Tele-Information, says:

Privacy is an interaction, in which the rights of different parties collide. A has a certain preference about the information he receives and lets out. B, on the other hand, may want to learn more about A, perhaps in order to protect herself. … [P]rivacy is an issue of control over information flows, with a much greater inherent complexity than a conventional "consumers versus business," or "citizens versus the state" analysis suggests. (Raicu, 2013) [34].

It is integral that ethics and privacy go hand-in-hand so that human dignity is upheld, which will go on to contribute to a vibrant and strong society. Privacy without ethics leads to threats to safety and self-determination, which has an adverse effect on the mental health of users.

Pappas *et al*. (2013) [31] finds there exists a negative correlation between concerns regarding privacy and the happiness of an individual. Subsequently, privacy concerns lead to a simultaneous increase in anxiety, which goes on to have a direct impact on the mental health of an individual.

Research such as Gwandure (2019) [14] finds the link between mental health and invasion of privacy, finding that instances of the latter occurring leads to emotional disorders such as stress, depression, and severe anxiety (Seligman & Diener, 2002) [37].

Most democratic societies uphold the combination of ethics and privacy to protect a person's right to privacy. Legislative reforms to protect this right include the proposed Open Democracy Act in South Africa (1996), the Privacy Act (1974) in the USA, the Data Protection Act in England, and even the Guidelines for the Protection of Privacy and Transborder Flow of Personal Data accepted by the OECD in 1980 (Collier, 1994) [7].

One of the more recent examples is the General Data Protection Regulation (GDPR). Passed in 2016, it has evolved into an integral part of EU privacy law and of human rights law, in particular, Article 8 of the Charter of Fundamental Rights of the EU. It puts forward seven principles to protect the privacy of EU citizens, as detailed in Articles 5(1) and 5(2) (European Parliament & Council of the European Union, 2016) [10].

Article 5(1) requires that the personal data of users should be:

a) processed lawfully, fairly and in a transparent manner in relation to individuals ('lawfulness, fairness and transparency');
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Article 5(2) requires that

"The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."

Most companies in the 21st century rely on user data to function. If they build their security and privacy framework on an ethical foundation, then they reduce the chances of facing legal liability and losing goodwill in the market in case of a data breach.

1.5 Ethical issues in online privacy

These are the main ethical issues as far as online privacy is concerned:

1. What to collect

Just because an internet user consents to share personal information does not mean it is unfettered access to everything they hold to be private. Clear lines must be drawn regarding what information (and how much) should be collected.

2. Confidential treatment

This is fundamental to the collection of user data – every piece of personal information disclosed must be treated as confidential and measures must be taken to prevent the theft of such data.

3. How will the information be used?

Once something is on the internet or in the hands of technology conglomerates, it can be used in a variety of ways. The same is true with user data, and with a majority of users feeling that they have no control over how their information is used, it remains to be seen how the data is utilized and whether it ends up to be detrimental for the users.

1.6 Ethical norms to tackle ethical issues

There are certain ethical norms that are applicable and can act as guidelines to address ethical issues when it comes to privacy. These are:

1. Truth

It lays down the need for the factual correctness and accuracy of personal information, thereby ensuring honesty, trustworthiness, and openness. Similarly, it ensures that the user knows how their data will be utilized as they are notified.

2. Freedom

Freedom is the main pillar of privacy. A person should have the freedom to choose what information they intend to disclose online, and be free from intrusions.

3. Human rights

Closely related to freedom, this is the explicit acknowledgement and protection of the privacy of an internet user. As a fundamental right, it also protects the user from unlawful intrusions.

1.7 Gaming and privacy: Why gamers are vulnerable

With video games constituting a large part of the entertainment industry, it was only a matter of time before privacy issues crop up. Unsecured Wi-Fi is one of the biggest privacy risks for gamers, since it exposes them to hackers. With the online gaming ecosystem evolving into an economy that often involves the exchange of real-life money and trading in virtual items, this has become one of the greenest pastures for cybercriminals.

Video games often contain microtransactions, where gamers have to use real-life money to purchase subscriptions, consumables, or other items. This involves trusting the game with personal information such as financial data (credit card details, for example), which can be stolen by hackers.

A survey done by a major security firm in the US found that 55% of gamers reuse passwords across accounts. This practice leaves them vulnerable to enterprising hackers, which often results in identity theft and hacked accounts.

Exposed card numbers may lead to hackers draining the bank of users or loss of in-game items, which a person may have invested hundreds of in-game hours and real-world dollars to get. The stolen virtual items can easily be exchanged for cash (N.A., 2015) [21].

Other reasons include malware, which are often spread via phishing methods. This kind of software intentionally disrupts the device to gain access to sensitive information and invade the privacy of gamers.

2. Materials and Methods

Research questions do exactly what their names suggest – they are specific inquiries which the researcher seeks to provide responses to. While objectives define the research, research questions provide a direction to it.

In the current study, the researcher seeks to answer the following questions:

1. Is privacy a myth or a reality in online gaming?
2. What, according to users, are the threats to their privacy as they play online games?

In any research, the methodology in an integral component. It can be defined as a logical, systematic plan that the researcher will undertake in order to solve a particular problem and ensure valid, reliable results that address the objectives of the research. Research methodology consists of variables techniques, but are broadly classified into two types - qualitative and quantitative.

Privacy, as discussed earlier, is an intangible entity. Thus, the researcher has resorted to qualitative methods for the purpose of the current study.

2.1 What is qualitative research?

Qualitative research techniques involve the collection and analysis of non-numerical data in order to better understand concepts or opinions. Techniques used in qualitative research include interviews, case studies, focus groups, questionnaires, and documents.

2.2 Methodology for the current research

For the purpose of the current research, the researcher has taken the case studies of three popular online games:

1. PUBG Mobile,
2. Pokémon Go, and
3. Angry Birds.

These three games have been chosen because despite being immensely popular at a time, their policies and practices regarding data collection and utilization made them the centres of controversies (which had more consequences). In addition, the researcher has interviewed five people.

Due to scheduling conflicts and lack of time, the interviews were conducted via Google Forms.

A mixture of case studies and interviews will be utilized to address the objectives and answer the research questions.

3. Results and Discussions

3.1 Case Studies

3.1.1 The rise of PUBG: Mobile and its fall from grace

PUBG: Battlegrounds (formerly known as Player Unknown’s Battlegrounds) became a quick hit after it was released in 2017. Originally launched for Microsoft Windows, the battle royale game clocked its official debut on Xbox a year later. In the same year, PUBG Mobile was released as a free-to-play mobile game version for both Android and iOS.

Developed by LightSpeed & Quantum Studio, a division of Tencent Games, PUBG Mobile was launched by various publishers – including Krafton, Tencent, and VNG Games – in multiple regions. Just like PUBG: Battlegrounds, the mobile version of the game tasted quick success to become the most-played video game of all-time and garnered a huge player base.

As of August 2021, it had 1.12 billion downloads and by May 2022, it grossed over $8.42 billion. This put it at the fourth position in the list of the highest-grossing mobile games, behind Honor of Kings/Arena of Valor, Monster Strike, and Puzzle & Dragons.

Despite reaching impressive heights, PUBG Mobile entered dire straits in 2020 as it ran afoul of the Indian government, or more specifically, the Ministry of Electronics and Information Technology (MeitY). After receiving numerous complaints and reports that PUBG Mobile, along with several other mobile apps, had been engaged in transmitting user data in an unauthorized manner to servers placed abroad, namely, China.

Under Indian law, this harvesting, transmission, and subsequent mining of data (of Indian users) and its use in profiling by foreign and hostile elements is a direct threat to the national security and defence, and by large, the sovereignty and integrity of the country.

Invoking its power under Section 69A of the Information Technology Act, along with the relevant provisions of the Information Technology (Procedure and Safeguards for Blocking of Access of Information by Public) Rules 2009, MeitY banned PUBG Mobile and a host of other Chinese apps in September 2020 (Ministry of Electronics and IT, 2020) [19].

Since then, PUBG Mobile has struggled to regain its foothold in the Indian market. In 2021, Krafton rolled out a version of PUBG Mobile specifically tailored for Indian users, known as Battlegrounds Mobile India (BGMI). In order to remain compliant to Indian laws, Krafton and PUBG Studios registered “PUBG India Private Limited” under the Ministry of Corporate Affairs, Government of India. Like its previous version, BGMI became a quick hit and surpassed 100 million downloads on the Google Play Store as of July 2022.

Nonetheless, it reportedly continued the same practice that PUBG Mobile was accused of – undermining user privacy by collecting and transmitting their data abroad to be mined and used for purposes such as profiling. Krafton admitted that it uses third-party solutions to provide several game features and that it shared “some” game data to said parties.

However, it maintained that sending data to servers in China was not in violation of its privacy policy, which entails that the game collect private information such as IP address, network type, available space, information about the device, its battery level, platform, carrier, WiFi strength, OS version, country code, and others.

Shortly after this, BGMI was blocked under Section 69A of the Information Technology Act, and it was removed from the Google Play Store and the Apple App Store.

3.1.2 Enter Pokémon Go and Niantic, exit user privacy

If there is one example of an online game tasting success soon after being launched, it is Pokémon Go. The augmented reality (AR) mobile game took the online (mobile) gaming industry by storm – in fact, reports suggest that it surpassed micro-blogging site Twitter, social networking site Facebook, and streaming giant Netflix in its daily popularity on Android. On iPhone and other Apple devices, it saw more downloads in its first week than any app that had launched before.

Its meteoric rise to popularity and helping users catch Pokémon while leveraging AR technology has often blinded users to the dark side of the game – the tremendous amount of personal data it requires from users to provide them with the authentic Pokémon hunting experience. Marc Rotenberg, the President and Executive Director of the Electronic Privacy Information Center (EPIC), described it as a “trove of sensitive user data” (2016) [36] in a letter to the Federal Trade Commission.

What makes the game all the more alarming is it poses an enormous security risk to every user who downloads and plays the game on their devices. In its bid to let users capture, train, and battle Pokémon in real-world settings, Pokémon Go tracks every piece of data related to users’ movements.

In its initial stages, Pokémon Go and its developer Niantic got access to the Google accounts of users, that is, unrestricted access to their contacts, email, IP address, search and map navigation history, deleting documents in Google Drive, and even private photos in Google Photos. And all of this would happen without the consent of the user, who simply logged on to the app through their Google accounts and did not receive any notification about the serious breach to their privacy.

While the company maintained that it did not sell or rent the personal information of users to third parties, a case of a data breach could easily have widespread ramifications as hackers would have access to a staggering amount of private information of users.

Understandably, a huge controversy was created when Pokémon Go and Niantic’s practices regarding user data and privacy (or the lack of it) were exposed. To make amends, Niantic drastically reduced the permissions needed to access the basic profile information of the Google accounts of users. But the damage was done by then.

While it can be argued that both the game and Niantic, which is a former Google company formed in 2015, managed to stay afloat and ride out the waves, subsequent years saw a steep drop in its numbers – it dropped to its lowest level of 65 million users after 2016, and while it rallied to increase that number to 133 million in 2018, the numbers fell sharply to 71 million in 2021.

3.1.3 An “angry” case study

A year after it rolled out in 2009, Digital Trends (Camp, 2010) [5] said that it was “one of the most mainstream games out right now.” More than a decade down the line, Angry Birds still remains one of the most enjoyable, addictive, and popular games of its time. What began as a simple casual puzzle video game by Rovio Entertainment soon led to a booming franchise that saw the game being released on personal computers and gaming consoles, merchandise, and even the release of two feature-length animated films.

Overall, Angry Birds, its numerous sequels, special editions, and its spin-offs went on to have over four billion downloads in all across all platforms as of January 2018. However, not all is sunshine and roses in what has appeared to be one of most colourful and unthreatening mobile games.

Edward Snowden, the former computer intelligence consultant who leaked highly classified information from the National Security Agency, leaked documents that marked Angry Birds as one of the “leakiest” apps that the National Security Administration used to access and utilize sensitive information of civilians.

While that did not stick, it was enough to sow the seeds of doubt. The fact that gameplay data is intricate by nature and people seldom understand exactly what information the game is gleaning from them, did not help matters. This resulted in the hack of Rovio’s Angry Birds website in 2014. At that time, hackers defaced the site with an image entitled Spying Birds, featuring an NSA logo. Rovio later denied that it collaborated with any government intelligence agencies, even though the leaks suggested that the NSA and its British counterpart GCHQ had obtained data released by Angry Birds.

In its privacy policy, Rovio lists the 43 data controllers and processors, including 14 advertising intermediaries, to which it sends user data. Three of them are likely to be violating the Children’s Online Privacy Protection Act (COPPA).

In February 2019, a study at UC Berkeley found that Angry Birds was among 17,000 Android apps that created and sent permanent advertising IDs. These IDs can later be combined to create more accurate activity histories, which would usher in an entirely new era of targeted advertising. Rovio declined to comment on the matter.

Two years later, Angry Birds made news once again, all for the wrong reasons. In August 2021, the company was taken to court by Hector Balderas, the attorney general of New Mexico. It alleged that the Finnish game developer resorted to illegal means to collect the data of users – more specifically, children who were yet to reach the age of 13. The lawsuit also alleged that the sensitive data was then sold by Rovio Entertainment to several third-parties. These parties would then go on to utilize that information for targeted advertising.

"Rovio monetizes children by surreptitiously exfiltrating their personal information while they play the Angry Birds Gaming Apps and then using that personal information for commercial exploitation," the lawsuit (Coble, 2021) [6] states.

3.2 Interviews

For the current study, the researcher interviewed a total of five individuals, several of whom have a presence in the gaming community, including ZuluKing, a popular content creator on YouTube. The interviews were held via Google Forms owing to scheduling conflicts and lack of time.

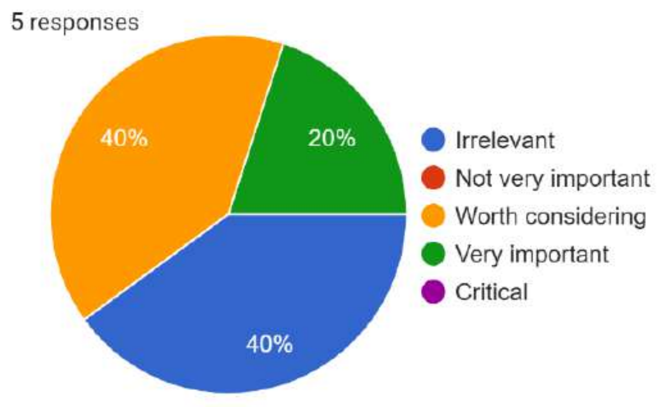

Chart 1: How important the reputation of the company in your decision to give personally identifiable information to them

When it comes to privacy amidst playing online games, several of the interviewees are of the opinion that the reputation of the company carries no value in their decision to share information that may personally identify them. With increasing user awareness, online games are skipping over asking users to share personal information, as is shown in Chart 2.

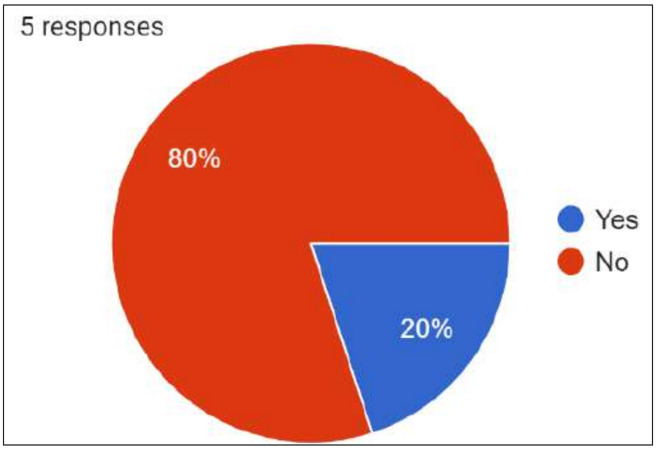

Chart 2: Have you been asked to provide/ share/ allow access to personal information (such as your name or location) when you play game.

As per the chart, only one out of five users have been asked to provide personal information while gaming. It is evident that if users do not have to, or feel inclined to, share personal information, then they will be less concerned regarding invasions of their privacy when it comes to playing online games. Chart 3 highlights the reasons why gamers might refuse to share personal information with the company, and exactly how important to them are the reasons.

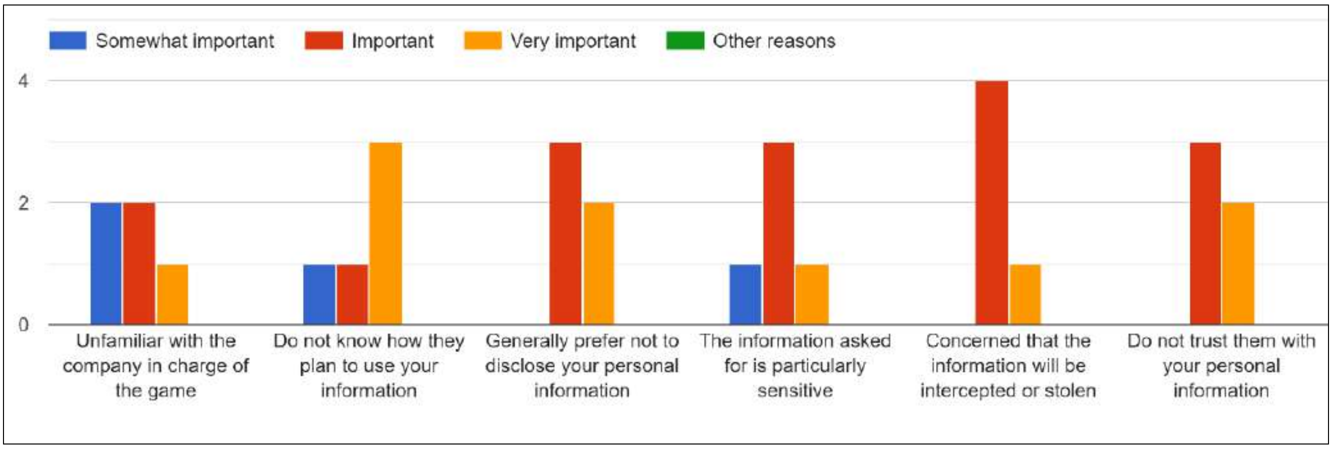

Chart 3: If you have refused to disclosed personal information, how important to you were the following issues?

Chart 4 builds upon the findings of the previous chart, highlighting the willingness of the interviewee to disclose personal information while gaming.

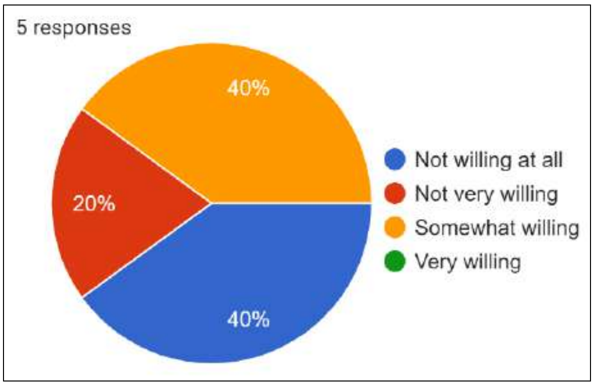

Chart 4: How willing are you to disclose personal information when you play online games?

On the other hand, Chart 5 highlights exactly how concerned the interviewees are about their privacy while playing online games.

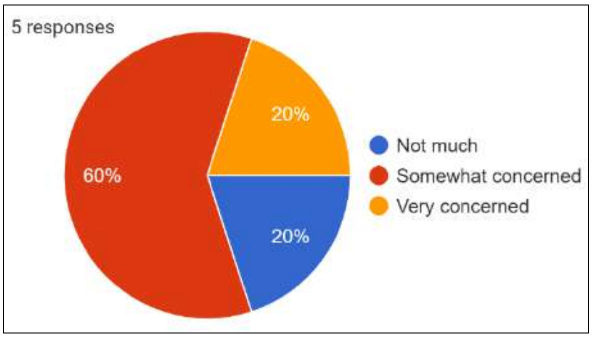

Chart 5: How concerned are you about the privacy of your information while gaming?

Apart from demographics and the above charts, several questions were asked to the interviewees, and the answers are as follows:

1. Interviewer: "Gaming companies should disclose what they intend to do with information collected from users." Do you agree with this statement? Give reasons.
Interviewee 1: Yes, it is personal data that should not be shared, just like if you told a friend something personal and didn't want it spread around.
Interviewee 2: I absolutely agree with this. Personal information is something that is starting to become equally important as the individual, if not more. In such cases, it is imperative that corporations make it clear as to what they intend to do with the data they collect.
Interviewee 3: Yes.
Interviewee 4: I agree. I think if they know my location, I'll get their dedicated server to play in, for my location.
Interviewee 5: Yes, because it's our information and we have a right to know how it's being used, and also, we need to have something to reference against in legal cases where an agreement might be broken.

2. Interviewer: What do you think should gaming companies do to better protect the privacy of gamers?
Interviewee 1: They just shouldn't need private information.
Interviewee 2: They could allow gamers to have a different name online, or have 2FA set up for the digital accounts.
Interviewee 3: Idk.
Interviewee 4: A feature to hide my name in game, while I'm streaming live.
Interviewee 5: Not ask for personal information.

3. Interviewer: Do you believe that companies and developers in charge of online games have a duty to preserve the privacy of gamers? Elaborate.
Interviewee 1: Yes. Just like a bank, or an insurance company, or a hospital.
Interviewee 2: They do! In the era of online activities, gaming entails one to share as much personal data as say, streaming movies or buying something online. In such cases, preserving the privacy of gamers is important not only from an ethical point of view, but also to create a sense of goodwill.
Interviewee 3: Lol.
Interviewee 4: They do have responsibilities. Because I'm doing in-game purchase often, and sharing information such as passwords, location and others, and these are sensitive elements of my personal life.
Interviewee 5: Yes, because they need to protect people who trust them.

4. What do you think are the threats to your privacy while gaming?
Interviewee 1: My safety.
Interviewee 2: Perhaps the biggest threat to online gaming

is having ones IP address or their financial details exposed.

Interviewee 3: Stream snipers.

Interviewee 4: My passwords, purchasing information, location

Interviewee 5: Companies sharing personal information or leaking it.

4. Conclusion

With the coming of the internet, maintaining privacy become infinitely more complex. As data became the key in driving the information age, it calls into question the ethical issues that tie in with online privacy. The case studies of Pokémon Go, Angry Birds, and PUBG Mobile have shown that unless the privacy policies of game developers are built on an ethical foundation, they will be the ones to suffer in the long run as both their business and goodwill will take hits.

It is thus imperative that video game companies utilize ethical practices in order to protect the privacy of gamers, so that both parties will benefit in the long run.

The objectives set for the purpose of the current research are addressed:

1. According to gamers, the greatest threats to their privacy while gaming include the disclosing of personal information such as their passwords, location, and purchasing and financial information (which games are likely to acquire via microtransactions).
2. The ethical issues and norms discovered in the literature review accurately reflect the reality – honesty, truth, and integrity are the key to preserving the privacy of online users (in this case, gaming). If companies are ethical in their policies to collect and utilize personal information and treat it in a confidential manner, taking proper measures to ensure that security breaches do not expose user data, then users will be more inclined to trust the companies with their personal data.
3. The final objective builds upon the previous one – the interviews conducted determined what the ethical responsibilities of gaming companies regarding user data are. As gaming companies take measures to preserve the privacy of gamers, which is their duty, they will generate goodwill among their customers (gamers).

The above points summarize the answers to the research questions set for the purpose of the current study. Measures such as 2FA (Two-factor Authorization) should be encouraged by gaming companies from improved account security, and they can provide the required framework and user support. And while privacy is not entirely a myth in online gaming, it is up to the companies to keep it that way.

4.1 Further scope and limitations

The further scope for studies on online privacy is huge. The research study can be extended to further discover the ethical issues regarding online privacy, video games, and social networking sites. The current study was limited by the lack of time – this can be amended in future studies where more methods such as focus groups and surveys are employed to drive more insights into the topic.

5. References

1. Auxier B, Rainie L, Anderson M, Perrin A, Kumar M, Turner E. Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information. Pew Research; c2019.
2. Baruh L, Cemalcilar Z. It is more than personal: Development and validation of a multidimensional privacy orientation scale. Personality and Individual Differences. 2014;70:165-170.
3. Britz R. Technology as a Threat to Privacy: Ethical Challenges and Guidelines for the Information Professionals. 1996;13(3-4):175-93.
4. Buchanan T, Paine C, Joinson A, Reips U. Development of measures of online privacy concern and protection for use on the Internet. Journal of the American Society for Information Science and Technology. 2007 Jan 15;58(2):157-65.
5. Camp J. Israeli Angry Birds satire goes viral. Retrieved from Digital Trends; c2010. https://www.digitaltrends.com/gaming/israeli-angry-birds-satire-goes-viral/?news=123
6. Coble S. Angry Birds Developer Accused of Illegal Data Collection. Info Security; c2021.
7. Collier G. Information privacy. Just how private are the details of individuals in a company's database? Information Management and Computer Security; c1994. p. 41-45.
8. Dhir A, Torshiem T, Pallesen S, Andreassen C. Do Online Privacy Concerns Predict Selfie Behavior among Adolescents, Young Adults and Adults? Frontiers in Psychology. 2017 May 23;8:815.
9. Durnell E, Okabe-Miyamoto K, Howell R, Zizi M. Online Privacy Breaches, Offline Consequences: Construction and Validation of the Concerns with the Protection of Informational Privacy Scale. International Journal of Human–Computer Interaction. 2020 Nov 25;36(19):1834-48.
10. European Parliament N. Council of the European Union, N. General Data Protection Regulation; c2016.
11. Golson J. Scientists just made a huge breakthrough in reducing plastic waste; 2021, April 23. Retrieved from Inverse: https://www.inverse.com/innovation/scientists-turn-plastic-into-oil
12. Goswami S. The Rising Concern around Consumer Data and Privacy. Retrieved from Forbes: 2020, December 14. https://www.forbes.com/sites/forbestechcouncil/2020/12/14/the-rising-concern-around-consumer-data-and-privacy/?sh=5aa5600d487e
13. Grove A. Andy Grove: What I've Learned. (Esquire, Interviewer). 2007, January 29.
14. Gwandure C. Life with Limited Privacy due to Housing Challenges: Impact on Children’s Psychological Functioning. African Safety Promotion: A Journal of Injury and Violence Prevention. 2009;7(1).
15. Kidder R. How Good People Make Tough Choices: Resolving the Dilemmas of Ethical Living. New York: Harper Collins; c1995.
16. Mason R. Four ethical issues of the information age. MIS Quarterly; c1986.
17. McCormick R. Hack leaks hundreds of nude celebrity photos, September 14. Retrieved from The Verge; c2014 https://www.theverge.com/2014/9/1/6092089/nude-celebrity-hack
18. Mekovec R. Online privacy: overview and preliminary research. Journal of Intelligent & Fuzzy Systems. 2010

Dec 14;34(2):195-209.

19. Ministry of Electronics, IT N. Government Blocks 118 Mobile Apps Which are Prejudicial to Sovereignty and Integrity of India, Defence of India, Security of State and Public Order; c2020.
20. Morris C. Massive data leak exposes 700 million LinkedIn users' information. Fortune; 2021, June 30.
21. NA. Data Privacy and Online Gaming: Why Gamers Make for Ideal Targets. Retrieved from Trend Micro; c2015; c29. https://www.trendmicro.com/vinfo/us/security/news/online-privacy/data-privacy-and-online-gaming-why-gamers-make-for-ideal-targets
22. NA. Digital Development. Retrieved from The World Bank; c2022. https://www.worldbank.org/en/topic/digitaldevelopment/overview
23. NA. Digital economy to see exponential growth to $800 bn by 2030: FM. The Economic Times. 2022;31:1.
24. NA. Oxford Learner's Dictionaries. Oxford; c2022.
25. NA. Privacy; c2022. Retrieved from Dictionary.com: https://www.dictionary.com/browse/privacy
26. NA. Privacy. Retrieved from Cambridge Dictionary; c2022. https://dictionary.cambridge.org/dictionary/english/privacy
27. NA. Privacy. Retrieved from Merriam Webster; c2022. https://www.merriam-webster.com/dictionary/privacy
28. Natividad A. An Introduction to Targeted Advertising; 2020. Retrieved from The Next Ad: https://thenextad.io/blog/an-introduction-to-targeted-advertising/
29. NG A. What Does It Actually Mean When a Company Says, We Do Not Sell Your Data? 2021. Retrieved from The Markup: https://themarkup.org/the-breakdown/2021/09/02/what-does-it-actually-mean-when-a-company-says-we-do-not-sell-your-data
30. OECD. Measuring the Digital Transformation: A Roadmap for the Future. Organisation for Economic Co-operation and Development; c2019.
31. Pappas I, Giannakos M, Kourouthanassis P, Chrissikopoulos V. Assessing emotions related to privacy and trust in personalized services. Conference on e-Business, e-Services and e-Society; c2013. p. 38-49.
32. Paul R, Elder L. The Miniature Guide to Understanding the Foundations of Ethical Reasoning. United States: Foundation for Critical Thinking Free Press; c2006.
33. Perkins E. Nothing gets deleted on the internet. Startups Magazine; c2020.
34. Raicu I. The Ethics of Online Privacy Protection. Retrieved from Markkula Center for Applied Ethics; c2013. https://www.scu.edu/ethics/privacy/the-ethics-of-online-privacy-protection/
35. Rosen J. The Web Means the End of Forgetting. The New York Times; c2010.
36. Rotenberg M. NA; c2016.
37. Seligman M, Diener E. Very happy people. Psychological Science; c2002, p. 81-84.
38. Singh J. Bizongo Data Leak Exposed Details of Customers Making Online Purchases: Researchers; c2021. Retrieved from Gadgets 360: https://gadgets360.com/internet/news/bizongo-data-breach-server-misconfiguration-amazon-flipkart-swiggy-zomato-customer-details-leak-2412565
39. Singh J. Flipkart's Cleartrip confirms data breach after hackers put data for sale. Retrieved from TechCrunch; c2022. https://techcrunch.com/2022/07/18/cleartrip-data-breach-dark-web/
40. Society TI. The Trust Opportunity: Exploring Consumer Attitudes to the Internet of Things. The Internet Society; c2019.
41. Spinello R. Ethical Aspects of Information Technology. New Jersey: Prentice-Hall Inc; c1995.
42. Stahie S. Spotify Hit by Yet Another Data Leak. Retrieved from Bitdefender; c2020. https://www.bitdefender.com/blog/hotforsecurity/spotify-hit-by-yet-another-data-leak
43. Stone EF, Gueutal HG, Gardner DG0, McClure S. A field field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations. Journal of Applied Psychology; c1983. p. 459-468.
44. Tene O, Polonetsky J. Privacy in the Age of Big Data: A Time for Big Decisions. Stanford Law Review. Retrieved from Stanford Law Review; c2012.
45. Wang Y, Genc E, Peng G. Aiming the mobile targets in a Cross-Cultural Context: Effects of Trust, Privacy Concerns, and Attitude. International Journal of Human-computer Interaction; c2020. p. 227-238.
46. Warren S, Brandeis L. The Right to Privacy. Harvard Law Review; c1890.
47. Westin A. Privacy and Freedom; c1967.
48. Westin A. E-commerce and Privacy: What Net Users Want; c1998.
49. Winston Strawn. (n.d.). What is the Definition of Online Privacy? Retrieved from Winston & Strawn LLP; c1998. https://www.winston.com/en/legal-glossary/online-privacy.html