# ETHICAL, SOCIAL, PROFESSIONAL AND LEGAL ISSUES INVOLVING THE SECURITY CONCERN OF ONLINE COMPUTER GAMES

AUTHOR: CHUKWUEMEKA MICHAEL NNAMDI INYA

## INTRODUCTION

The advancements in information system technologies into today's society have given rise to several concerns regarding data security and privacy. However, these concerns relate to protective measures taken with respect to digital privacy and the protection of unauthorised access to databases of information. Regarding information system technologies, computer games have been designed in such manner to collect, process and store personal data of the gamers. This raises several concerns on the security measures taken to ensure the security of

personal data. Mainly, computer games appear to be a source of entertainment, especially for younger generations. However, far beyond fun, they have been for decades as one of the major computer applications with far-reaching implications, especially regarding security. According to Briggle (2008), there have always been copying protection mechanisms in the console games, but the bulk of the security effort of game retailers has been focused on locking in customers to their hardware.

As technology advances, many computer games as well as security risks have advanced and have become a prevailing factor in the computer gaming industry. Recent security breaches have proven that security risks can cause damage within the computer game industry, especially regarding the user data that is transmitted on the consoles. Top computer game industries such as Sony, EVE online, League of Legends, Bethesda, and Minecraft have experienced security breaches in recent years. However, this essay tends to investigate the security issues in online-computer games and the ethical, social, legal, and professional associated with processing and management and personal data.

## ETHICAL ISSUES

The rate at which personal information is transmitted between the gamers and the gaming organisations raises ethical concerns regarding the integrity, openness, transparency, and ethical responsibilities of the game designers to ensure adequate security of personal data. Also, it examines how gamers use their ethical values in gameplay. However, ethics in computer games can be analysed under Utilitarian, Kantian, and Virtue ethics, which relates to the personal character towards computer games. According to Briggle (2008), computer games are ethical subjects, while the game players are the ethical agents. Therefore, the ethics of computer games should be perceived as a complex network involving responsibilities and moral duties. In this regard, the players must not be considered passive amoral creatures as they relate, reflect, and create with ethical minds. So, computer games are regarded as moral objects based on their design and the manner at which they create an experience of their design. In other words, the design of the system to influence the ideas and dispositions of the players is a significant concern (Bissett et al., 2004).

However, with respect to security, ethics plays an important role, especially in managing personal information. According to Castronova (2001), security levels in computer games consist of legal, social, technical, and organisational. In most cases, game designers lack moral principles to protect gaming consoles from unauthorised access, disruption, modification,

disclosure, and use. According to Kant's theory of ethics, an action cannot be justified to be right or wrong based on its consequences but based its morality (Duquenoy, Jones and Blundell, 2008). In other words, the incapability of the game designers in ensuring that the computer game information system is well secured from unauthorised access is unethical. This action cannot be justified based on the consequential theory which states that an action can be ethical when it benefits to immense population integrity, availability and confidentiality are meant to be the primary concerns regarding the security of the information system. Hackers are the major threats to the security of computer games as they disregard and violate moral principles to manipulate, use and gain unauthorised access to information (Buchanan and Ess, 2005). According to Kant's theory of ethics, this act is wrong because the information stored on the gaming networks requires to be well encrypted and protected against malicious attackers.

However, in an ethical dilemma where there is an issue with the gaming network and the only way to rescue the system is to gain unauthorised access to the system to manipulate and use the information, it can be argued following the consequential theory of ethics to be right. Although hacking is ethically wrong under ethics in information security, it can be justified when the benefits supersede the consequences. An example of a similar scenario is the case of a Dutch hacker, who gained authorised access to computer material, and copied personal data but was not caught. However, the hacker testified that the act was carried out to publicise the vulnerabilities of the system and not to use the information. In such a case scenario, the action is ethical because the intention was for the benefit of the organisation and the clients to see the vulnerabilities of the system and intensify their security systems (Nelson, 2002). In the case of computer games, such cases of hacking have been a prevailing act, but if the intention of the hacker is like that of the Dutch hacker, the action can be justified to be ethical.

The persuasiveness of computer games also raises ethical concerns due to its ability to influence people's attitudes and behaviour. According to Fogg (2002), such computer technologies can be more persistent than a human being, manage a high volume of data, offer greater anonymity, use various modalities to exert influence, can be used where humans might not be allowed, and can easily adapt to increased demands. With such a level of manipulation and cunning behaviour of the technology, it is unethical according to Kant's theory. However, considering the intended benefits to the larger population, it can be justified following the consequential theory. For instance, the computer game "America's Army" that was designed for recreating "the US Army for the benefit of the younger citizens" (Zyda, 2003).

The issue of selling personal data to third parties raises ethical concerns on the integrity of the game designer in securing the data given tot by the customers on the virtue of trust. According to Kant's theory, this is unacceptable and unethical to sell data from statistics of gameplay and other personal information to third parties without the consent of the gamers. Although it can be argued under the consequential theory if the intention of the action surpasses its consequences, however, the consent of the players must be required for such transfer of personal data according to the ethical conduct guiding the professionals.

## SOCIAL ISSUES

From a social perspective, security issues in computer games pose challenges alongside the benefits. For instance, besides the pleasures and fun players derive from playing computer games, there are health and educational benefits. According to Griffiths (2003), there are computer games that are designed, especially for rehabilitation and habituation. Such games defeat security threats as users look more on the benefits than the unseen risks. Some computer games have been reported as great tools for improving the teaching of eye-hand coordination and the visual-spatial ability for some impaired individuals. Also, some computer games help in fostering creativity, help children become more comfortable with computers and technology more than their parents or other folks that do not own computer games. In the light of the social benefits, Dodig-Crnkovic and Larsson, (2005) mention playing computer games helps players especially teenagers to develop a higher level of literacy, collaborative skills, communication, logical think, and strategies for solving critical problems.

For instance, some games require players to apply different strategies to solve a problem, and this influences their behaviours in real-life scenarios. Generally, computer games influence the behaviours of the player because it is designed cunningly to mimic the players to make them feel the reality of the game. This can be seen as a social challenge because some teenagers tend to get addicted to the games, and the impact tends to affect them psychologically. Ke (2011) mentioned that some mental cases among teenagers are either influenced by drugs or addictiveness to computer games. While some teenagers are benefiting from computer games, some are being negatively influenced as they spend much time and money on games than they spend on their studies. In most cases, teenagers are found in a game house during school hours because they are addicted to computer games, so they direct more importance on the games than their education or social activities.

However, one of the biggest threats to information security in the social context is cybersecurity risks. Despite the social benefits of the computer games, most teenagers overlook the security risk involved with the system regarding the measures taken by the gaming industries to ensure adequate security on the information transmitted through the gaming networks. Most of the computer games are played online, so there are several security risks such as disclosure of information and cyber-attacks. According to Gotterbarn (2010), the computer game industry is a valid target for cybercriminals because gamers give out sensitive information such as personal credit card details which is used to purchase games and unlock features. However, it is not only credit card detail that is targeted but the personally identifiable data collected by the game designers such as a home address, date of birth, and personal interest information. These details are incredibly lucrative to cybercriminals Karlsen (2016). As gamers come from a wide range of groups, their information is very attractive as well as their gaming accounts and in-game purchases.

According to Shaffer (2006), the gaming industries are not targeted by cybercriminals because of money or fun, but there have been many issues that connived with state-sponsored disruptions and other social insurgencies. Likewise, in-game economies have substantially provided a precursor to cryptocurrency, so even though virtual money that is earned in-game cannot be used in the real world, it is still valuable to the players. Thus, a computer game account with a massive number of in-game currencies can fetch high real-world prices, and it is a major target. For instance, a moderator for one of the longest-running computer games, RuneScape recently exploited his elevated privileges to steal virtual money worth 45 billion in-game coins with a real-world value of $100, 000 from gamers. Additionally, many computer games are sold, published, and authenticated on online distribution platforms like Origin, Steam, and GOG Galaxy. Most times, players manage all or most of their games through a single account, and long-term users of Steam have libraries containing numerous games, and the company usually allows gamers to own and trade supplementary virtual items like stickers, wallpapers, and in-game cosmetics. In many cases, hackers have gained access to Steam's inventory to steal items and accounts on Origin.

As the gamers play, information concerning their behavioural patterns, media engagement, location, their skills, playing patterns and strategies achieving tasks are being captured by the gaming industries and used to develop more games. Most often, hackers are mainly interested in the accounts of the players due to the amount of sensitive information collected by the game industries.

## PROFESSIONAL ISSUES

Regarding data security of computer games, there are responsibilities and actions required from the IT professionals in the gaming industry to ensure adequate security measures are employed. However, the BCS Code of Conduct provides some guidelines concerning the ethical positions of the game designers in some dilemmas. For instance, section 3 of the BCS code of ethics reprimands IT, professionals, to take adequate measures to protect the personal data from deliberate access or improper use. In other words, the professionals in the game industry must be competent enough in terms of security to protect the information of the gamers from malicious attackers or hackers (Gotterbarn, 2010).

Regarding professional competence and integrity, the BCS code admonishes IT, professionals, to "avoid injuring others, their property by malicious act", there has been cases where professionals in the gaming industries carry out operations that will affect the gamers such as the case of RuneScape where a professional intercepted the in-game currencies of the players and sold for real-world money. So, the professionals must possess competency and integrity towards personal information. Similarly, Section 3 code of ethics mentioned than IT professionals are duty-bound to "carry out their professional responsibilities with due care and diligence following the requirements of relevant authorities".

Under section 2 of the IEEE code of ethics, game designers are required to treat everyone fairly without any discriminatory act such as race, age, religion, gender, ethnicity and disability. Some computer games are premeditated to be played by only males and not females, and in most cases, games discriminate based on race or colour from the way they were designed. So, game designers should desist from unfair practice while creating computer games (Dodig-Crnkovic and Larsson, 2005).

Due to the global coverage of the computer game industry, intellectual property right has become a necessity across many jurisdictions. Although intellectual property is a legal matter, the duty of the professionals in such cases has become a major professional issue because some of the contents of the games are derived from the gamers especially artworks or images, music, and sounds. In this regard, the International Game Developers Association (IGDA) has provided ethical guidelines which require game designers to "seek civil rights to ownership of contents created with respect to intellectual property rights" (Karlsen, 2016).

Many computer video-games have been miss-rated for their benefits, and some other computer video- games are miss-rated accidentally as well. The Entertainment Software Rating Board

(ESRB) has miss-rated the best-selling ‘Elder Scrolls IV: Oblivion’ game as ‘Teen’ and then they have re-rated it as ‘Mature’. The customers who would have already bought the game would have been affected by this professional issue caused by its miss-rated content. This has breached BCS’s code of conducts under Public Interest- Section (A) and Under Duty to the Profession- Section (A). In this case, they have been only concerned about their business benefits, and they have neglected the concern towards the public. Another critical concern about professional issues is when creating computer video-games, do the game developers follow the professional code of conducts. Vitally some online computer game developers design their games to address various hidden things (Hartmann, and Klimmt, 2006).

## LEGAL ISSUES

In the case of information security in computer games, game designers should be liable for the information of their customers (gamers). Thus, they are under a legal obligation to ensure data of their gamers are well secured, especially from hackers or third parties. Most times personal data from statistics of use are being sold to third parties who use the data to design appealing gamers for the customers, but this must be done following the required regulations that permit the use of data in specific terms. For instance, the Data Protection Act 1998 states that personal data must be processed lawfully and fairly in a transparent way about the data subject. So, without a statutory justification, personal data should not be processed unlawfully. The regulation also stated that organisations must ensure clear information is provided to customers concerning how personal data will be used and who it will be shared with rather than rely on an information that is hidden maybe at the back of the console (McGraw and Hoglund, 2007). However, if there is any breach of this regulation, it is the right of the affected person to seek compensation for any distress the action might have caused. Section 6 of the EU GDPR, it states that “personal data must be processed in a way that it ensures appropriate security” this includes the protection against unauthorised or unlawful processing of data.

Considering the issue of hacking, which is prevalent in computer games, the Computer Misuse Act (1990) provides some regulations regarding some criminal offences such as unauthorised access to computer material, and unauthorised modification of computer material. Regarding unauthorised access to computer material such as hacking where a hacker makes use of the system without permission, the law subjects such person to be tried in a Magistrate’s court and such act carries a penalty of up to six months imprisonment or a fine of £2,000. For some issues such as stealing contents of games or information such as credit card numbers, it is viewed as a more serious offence under the section 3 of the Computer Misuse Act; such crime will be

tried before a jury with a severe penalty which is five years imprisonment and an unlimited fine.

However, in the case whereby a hacker or anyone gains access to the system containing personal data of the gamers, and then copy some data or all to another system, such person is liable to prosecution not only under the Computer Misuse Act but also the Data Protection Act of 1998. So, there are strict regulations to mitigate such issues of hacking or gaining personal access data without permission. There are other regulations that pertain to computer games such as the Equality Act 2010, which advocates against direct and indirect discrimination practices involved in computer games. Human Right. The UN Convention on the Rights of the Child requires the game designers "to protect the child from all forms of physical or mental violence" the question relates to the responsibility of someone in such context.

The issue with intellectual property rights in the game industry requires legal protection for copyrights, which includes software/coding, films, text, artwork/images, and gameplay. In this regard, Section 4 (1)(a) and 4 (2) of the EU Practical Law outlines specific laws that are mandatory for gaming organisations. Nelson (2002) reports that game consoles often contain hardware-based recognition systems that prevent the illegal use of unauthorised copies of computer games or games that are locked by region to be played in another territory. However, there are several manipulations in this regard as gamers make use of modification chips to circumvent the recognition systems to play illegal games purchased from a different geographical location from that of the console. In such cases, the Copyright Directive requires all the states under the EU to provide adequate protection against any form of circumvention and seeks to prevent the manufacture, import, sale, distribution, rental, or being in possession of any device that; "have the purpose of circumventing, are primarily designed to circumvent, have limited commercial use other than for circumventing". These effective technical measures cover both portable video games with protections.

## Vulnerabilities and Limitations

In terms of vulnerabilities, there are many computer games which are usually leveraged by hackers. A preliminary assessment of the vulnerabilities and limitations of the system found that most computer game companies operate on a variety of networking devices that usually combines Cisco and other networking components from various manufacturers. However, the networks typically comprise of fully functional TCP/IP LAN networks while some bigger companies operate a WAN integrated network that connects with their facilities worldwide.

However, for a company in two locations, it is risky if there is any failure in trying to connect each of the locations securely. Most of the video game companies run a complete MS window domain with a fully integrated active directory domain; also, they often run an Exchange server specifically for e-mail. So, with all the servers running the MS Server operating system, risks can be associated mainly to the operating systems. There are other vulnerabilities such as risks with the enterprise system hardware, and software. Online computer games are not just played by kids alone, and it's been played by individuals of a different class, a game player can be a politician or a company director that has access to useful information, so it compromises organizations and individuals' computers in attacks. Online computer game servers are always revolving around competitions between different clans, by people who want to cheat to increase their game positions illegally. Therefore, game companies spend more time and resources in getting anti-cheating solutions than to improve the security aspects of gaming. Game companies care more about cheaters than the individuals exploiting vulnerabilities on the systems of the gamers. The limitations are updates cannot be done to an online computer game without an internet connection; the game's patches cannot be downloaded without an internet connection. Also, online computer games must be played over an internet connection, and viruses on the gamers' system may affect the gameplay on the system.

## CONCLUSION

This study highlighted the ethical, social, professional, and legal issues related to the security of computer games. It was found that the role of the IT professionals to understand the ethical action to take in some dilemma and the legal directives that should be followed to ensure personal data is well secured and respected. Following the findings, the fun and pleasure derived from the computer games are no doubt beneficial to the players and the society, but farther than that the security issues are very glaring, especially with the hacker. So, gamers should endeavour to apply professional conduct and order to the profession and to the organisations to promote the better use of the information system.

However, to minimise liabilities, reduce risks found in the information security of computer games, the practitioners must; understand the existing legal environment, keep gamers informed of changes, stay updated with laws and regulations, and watch for new issues that will emerge.

# REFERENCES


Briggle, A., 2008. Real friends: How the Internet can foster friendship. *Ethics and Information Technology*, *10*(1), pp.71-79.

Bissett, A., Parry, P., Ritchie, I., Steele, B. and Vacher, P., 2004. Addressing Ethics in Entertainment Software Development. *ETHICOMP 2004*.

Briggle, A., 2008. Real friends: How the Internet can foster friendship. *Ethics and Information Technology*, *10*(1), pp.71-79.

Bcs.org. (2019). *British Computer Society*. [online] Available at: https://www.bcs.org/upload/pdf/conduct.pdf [Accessed 6 Apr. 2019].

Buchanan, E. and Ess, C., 2005. Introduction: The Ethics of E-Games.

Boyle, E., Connolly, T.M. and Hainey, T., 2011. The role of psychology in understanding the impact of computer games. *Entertainment Computing*, *2*(2), pp.69-74.

Castronova, E., 2001. Virtual worlds: A first-hand account of market and society on the cyberian frontier.

*Data Protection Act 1998*. [online] Available at: https://www.legislation.gov.uk/ukpga/1998/29/contents [Accessed 29 Feb. 2019].

Dodig-Crnkovic, G. and Larsson, T., 2005. Game ethics-Homo Ludens as a computer game designer and consumer. *International Review of Information Ethics*, *4*(12), pp.19-23.

Duquenoy, P., Jones, S. and Blundell, B.G., 2008. *Ethical, legal and professional issues in computing*. Cengage Learning EMEA.

Egenfeldt-Nielsen, S., 2011. *Beyond edutainment: Exploring the educational potential of computer games*. Lulu. com.

Gotterbarn, D., 2010. The ethics of video games: Mayhem, death, and the training of the next generation. *Information systems frontiers*, *12*(4), pp.369-377.

Griffiths, M.D., 2009. Online computer gaming: Advice for parents and teachers. *Education and Health*, *27*(1), pp.3-6.

Hartmann, T. and Klimmt, C., 2006. Gender and computer games: Exploring females' dislikes. *Journal of Computer-Mediated Communication*, *11*(4), pp.910-931.

*Human Rights Act 1998*. [online] Available at: https://www.legislation.gov.uk/ukpga/1998/42/contents [Accessed 1 Mar. 2019].

Ieee.org. (2019). *IEEE Code of Ethics*. [online] Available at: https://www.ieee.org/about/corporate/governance/p7-8.html [Accessed 7 Apr. 2019].

Karlsen, F., 2016. *A world of excesses: Online games and excessive playing*. Routledge.

Ke, F., 2011. A qualitative meta-analysis of computer games as learning tools. In *Gaming and Simulations: Concepts, Methodologies, Tools and Applications* (pp. 1619-1665). IGI Global.

Luck, M., 2009. Crashing a virtual funeral: morality in MMORPGs. *Journal of Information, Communication and Ethics in Society*, *7*(4), pp.280-285.

McGraw, G. and Hoglund, G., 2007. Online games and security. *IEEE Security & Privacy*, *5*(5), pp.76-79.

Nelson, M.R., 2002. Recall of brand placements in computer/video games. *Journal of advertising research*, *42*(2), pp.80-92.

Shaffer, D.W., 2006. *How computer games help children learn*. Macmillan.
Sicart, M., 2011. *The ethics of computer games*. MIT Press.

Sicart, M., 2013. Moral dilemmas in computer games. *Design Issues*, *29*(3), pp.28-37.