**MODULE TITLE: IT ETHICS AND LAW**

**ASSIGNMENT TITLE: THE VERDICT OF STEAL CHILDREN'S PRIVATE DATA ACROSS SOCIAL MEDIA PLATFORMS**

**Table of Contents**

[Abstract 5](#_Toc132804774)

[Key Words 6](#_Toc132804775)

[Introduction 7](#_Toc132804776)

[Social issues and impact 7](#_Toc132804777)

[Economic issues 8](#_Toc132804778)

[Technological impact 9](#_Toc132804779)

[Ethical Issues in using social media Platforms 10](#_Toc132804780)

[Legal Causes and Legislations 11](#_Toc132804781)

[Conclusion 13](#_Toc132804784)

[Reference List 14](#_Toc132804785)

# Abstract

This study would address the process of stealing the children’s private data and developing the suitable planning to combat the situation. In accordance to this social issues and impacts have been assessed in this study by focusing on the social impact identification as well. In addition, identification of the economic issues are also identified for the risk minimization process by aligning to the application of the Data Protection Act 2018. In addition, the ethical issues in application off social media platforms also have been assessed for the formulation of the cyber bullying protection concern. In addition, the legal cases are also assessed here considering the children data protection process and development as well.

# Key Words

Children private data, social media platform, violent photos and trafficking photos, Cyber bullying, Data Protection Act 2018, deployment of technologies, economic condition prevents.

# Introduction

In progressing to the modern era, the usage of IT and computer-related facts and technologies must be known to everyone. Thus in using them there needs to be a few laws and rules to be followed and developed by the governments. This is required to provide protection and balance in society. Ethics is smooth to be judged by society or organizations to prove what is right or wrong. The context of the study will cover the verdict of whether it is right or wrong to steal children’s private data from social media. The assignment will cover the social, economic, technological, and ethical issues that to use within social media platforms.

# Social issues and impact

Children in their growing stages and along with this modern age are immature to take over any critical situation. Children at their mature age have just started liking shiny things and found something that gets them interested is talking to someone through social media. There are many good impacts of social media and bad impacts as well (Sufi *et al*., 2022). Children can learn new things from social media and thus by connecting with friends and their community group teachers or educators they can learn and share useful things through social media. The bad impacts thus highlight their performance to deliver malware that can slow down the computer attack and thus clicking on adaptive advertisements on social media helps to steal sensitive data.

The impact of privacy thus takes place by enabling the collection of private data. Social media platforms that are enabled to collect data about the users thus get the data leaked from cookies, third-party apps, search engines, and other sources. Social media gives a negative impact on the behavior of depriving kids of the imprint causes and social cues that they would usually learn through the person in communication. It is unethical to steal children's private data across social media platforms. Children are immature to know and understand the privacy that should be maintained using social media. Through social media, children can get victimized by cyberbullying, which is one type of blackmail while hackers steal the information of children through social media. Hackers morphed one particular photo or video of children to cyberbully them through social media (Obermayer *et al*., 2022). Social impacts thus have on youths about their post and content that they share on social media inviting the risk of getting their photos morphed.

It is very dangerous for youth to share such intimate photos with them and thus sharing the calling number is visible to everyone. In addition to cyberbullying, children often fear facing society if their private photos and information gets leaked to hackers or others. Problematic changes in their behaviors appear to them that increase anxiety, self-esteem, and belief. Parallel to the positive impact children are likely to get trapped by the negative impact thus getting them to be under the pressure of cyberbullying (Crocco *et al*., 2020). Children with increased excessive technology are thus used to normalize social behaviors like rudeness and bullying. This always happens online and the main motto of the unethical hackers is to extort some money from the children somehow that would make them the cost of spending the labor on them.

# Economic issues

It is quite obvious that children of very small age are so immature that they fall into the trap of scammers without knowing. Unintentionally they have fallen into the trap of scammers thus losing so much money due to cyberbullying. The economic condition of many children at their immature age is not so good. Few parents give money to their child's hand and few won't, thus they fall into the scammer's hand to forcefully steal or beg money from their parents to satisfy the scammer's needs. With a smaller amount of data that is scammed, scammers from children try to scam larger data or they try to steal money from the children's houses.

Scammers can find enough information about the victim, especially from children, through social media. According to the Data Protection Act 2018, the issues and loopholes are connected through protecting the data of every individual. This can help to protect the law that can be used to mitigate the risk when using social media. The economic condition prevents the deployment of technologies that are related to new facilities. This would be helpful for children and many such adults also to protect the data and social media accounts (Richard *et al*., 2021). Profile locking systems have been initiated by Facebook to protect and hide confidential information of any individual or users to see the image of the users also.

Introducing AI in the latest technologies, scammers are using them also to make up for any such disadvantages that aren't responsible for the guiding system to have characteristics of appropriate gestures. However, it is typical to be mentioned the impacts of the economic condition that every individual must afford due to the introduction of AI-based facilities. It occurs by the substitute of human labor that is taken with some aspect of the work. It promotes the AI system that automates the tasks to drive off performing simulations of stealing and morphing children's data. The current trends of scenarios could be included with the responsibility for the guidance that might use gestures for the emotions taken from different scenarios.

# Technological impact

The technological impact that comes under IT ethics and law thus might be utilized to maintain the amalgamation of using different components. The Key components of technological features have the abstraction for AI concepts that might transform with reality. The usage of technological features in stealing children's private data from social media platforms. Thus it is not ethical to steal private data from children using technological means thus to bluff the children for the sake of stealing money and extortion (Banet-Weiser, 2021). Cyberbullying is very much common nowadays with security threats and massive investments the capital into the development of AI that have made novel technology. Nowadays children are very technologically well advanced which is commonly used in makeup for producing promising results.

The self-driven facilities are to be taken away with the phenomenon of luring advanced technological facts with automation and human capabilities. Technology thus can create positive and negative impacts on everyone's life similar to a child also. It is independently considered to be developed in the social skills for health, relationships, and overall ability to focus (Silver *et al*., 2019). This might be used to develop the learning notes for the skills of the children in developing any social situations. Technology thus furthermore aided with the evolution of social media usage thus taking place on the various voiceover communication, messaging applications, and social networks to impact on the misuse of stealing away of children’s data.

Teenagers have an impulsive nature thus being bold enough to post intimate pictures on social media. A technical feature thus detects any intimate pictures and informs the technical team of any social media apps to delete the bold pictures of someone especially children according to the data that gets leaked unintentionally in social media. Excessive use of internet usage thus influenced children and teenagers to be used and likely transform by reducing the amount of sleep that they get at night (Joshi and Patwardhan, 2023). It thus results in the children's sleep deprivation which can result in cognitive problems that would be trouble in focusing and deficiency of memory.

Media and communication by advances from social media thus take palace with the technological effects that would be making it quite easier to have for quicker and more efficient. It thus allows the track for the conversations to provide a better understanding of social media services. Technology also makes it easier to gather customer insights while stealing any data from a child’s social media account by alluring them through technological means. The impact of information thus takes place with the marketing tactics, with the facilitation of intercepting children's privacy thus indirectly affecting their parents' lifestyle. Social media thus affects teenagers by the negatively limiting usage of direct contact with their peers by encouraging an instant use of comparison. It can lead to a life of children their adolescent age with low self-esteem and depression and anxiety.

# Ethical Issues in using social media Platforms

The ethical issues in using social media platforms thus have positive distinctive personal information that is about the clients with breaches in confidentiality. According to the data protection act 2018, ethical considerations are taken to protect children's data with highly secured privacy (Blackwell *et al*., 2019). It is of aviation and confidentiality that social media accounts cannot be opened below 18 years but few teenagers and youngsters are trying to become smart to open a social media account at an early age to avoid becoming victims of cyberbullying (Data Protection Act., 2018). It would be wise to not spend so much time on social media that is used for spreading information about the information that is related to a certain race and religion.

This is useful for stealing information to avoid conflict with others that are being used for uploading violent photos and trafficking photos. If a morphed photo is uploaded by someone, then social media teams are quick and active enough to get deleted it within a few seconds and won't let it get published (Van Dijck *et al*., 2019). Private data of children especially get leaked by their own mistake and consequently, the parents of those children get affected. Social media can reveal information that can be taken for results with privacy breaches if not managed properly by users. The ethical issues that thus tend to be avoided in minimizing that will cause physical emotional harm to participants.

It thus makes the participants aware of any potential harms before information. This can be taken for something which seems to become on social media. Negative posts thus tend to have against the person with the person to demoralize by the cyberbullying. This can be true with the social issue that affects the mental health of the person to be involved. The use of social media thus defines for criminals to become and a real social issue. Cybercriminals are also using social media to get personal information about the users which may be used to break into accounts for stealing personal data.

The ethical consideration is using social media platforms that thus allow the users, especially children the expansion of use replicas of any private data so that children won't get any clue that their data is being copied. In this way, the investigator would not get any trace of the scammer's whereabouts to get the victim out of danger (Benyusz and Hulko, 2021). Thus children must be aware of using social media carefully, as prevention is better than cure. The data of any person, especially children's data, is thus protected with high-security purposes according to the Data Protection Act 2018. Thus a child must be well-guided to use social media very carefully.

# Legal Causes and Legislations

***Legal Cases 1***

The first legal case about the verdict was to steal of children's private data from social media platforms. Campaigner ***“Duncan McCann”*** had lodged a complaint in 2015 about the videos of children that are going viral where hackers have been watching what they have been watching on it. Social media YouTube has invested in using and protecting families. This has been included in treating children's content that went through even on an adult's account. Hackers give access for the children to such dull websites which children get more attracted to view stealing their information (Data Protection Act., 2018). It remains and continues engagement with the priority of work which is used for key stakeholders that are included by children in maintaining child protection experts. The social media platform is owned by the US tech giant Alphabet which is issued by the parent company Google. “***Mr. McCann”*** says plenty of children watch YouTube content on family devices that can be used where the data can be gathered by default thus it is not registered as a children's account.

Thus ultimately of the children's wrong steps their family members also get convicted of getting their information stolen from social media (Computer Misuse Act., 1990). Mr. McCann is acting in a personal capacity that might be working with the campaign group which is being championed. The best way to ensure that the data for the adults are properly used is believed to be the first test of ICO children's code. In 2019, YouTube is said to be fined 170 million USD which will make the US regulator for violating children's privacy laws. This is being followed by the accusation that the data was collecting information where the children under 13 were convicted and found to leak their private information unintentionally. Children's data stolen from YouTube has not admitted to taking responsibility that it did fine and also changed its business practices as a result.

The Children's Act 1989 has been levied in this case where the video and private data of the children have leaked through YouTube and thus it attracted lakhs of views within 1 hour. Comparatively, children's data are accustomed to morphed pictures that are used to face similar accusations in the system. There seem to be no defects in the interactions which have built with the decision-making abilities (Children Act., 1989). It must be claimed that it needs to prove the balance for the probability of the developers being neglected by the duty of care. It is being taken with a decision that will make it difficult to prove the victimized condition of young children. Thus due to parents and their child’s negligence, this leaking of private data occurs.

***Legal Cases 2***

In the next case, children’s private data gets leaked and stolen across social media. Google had agreed to pay a sum for the settlement with the ***“Federal Trade Commission”*** (FTC). Without any parental control, the video streaming site had been accused of collecting data for children by alluring them and stealing them unknowingly. The FTC data we used to target the ads on children contravened in 1998 under the ***“Children's Online Privacy Act”*** (Coppa). FTC chairman Joe Simons started making an excuse for YouTube's violation of the laws. Furthermore, he added that by complying with the Coppa Google had to refuse the verdict to acknowledge the main parts of the conviction set out by YouTube service was directed at children.

The FTC demanded that YouTubers make any content for children that must be notified that the videos of them must be subjected and treated to the Coppa rules. Furthermore, Google and YouTube are now required to be more important and to be more open about data protection gathering practices (Children Act., 1989). Ms. Wojcicki stated that it had taken what it could make in addressing children for watching videos without any parental supervision. She also suggested that social media must be used by children also under parental guidance. She also said the firm would stop targeted ads based on the users who watched the children’s video. The case had defined that it will treat data from anyone watching children’s content on YouTube as coming from childhood regardless of the users (Data Protection Act., 2018). It is implied that it means that hackers would limit the information on collecting information and thus the confidential videos of children thus making the kids online be what is needed the support for the operation of services.

***Legal Cases 3***

# Computer Misuse Act 1990

# In 1990, the Computer Misuse Act 1990 has been introduced considering the fact of denying the risk regarding the wrong application of this by the children. In 2016, a 17 years old boy had an incident regarding the matter of hacking the information of Talk-Talk. In Norwich Youth Court, this case has been heard. Herein, the issue of massive personal data breach has occurred and as a result £ 4,00,000 amount has to be provided as a fine. This act summarizes with the criminalize performance of data hacking and installing of malware to steal information from the computer. The 17 year old boy’s data have been restored, thus it hadn’t been published and it is protected against the Data Protection Act 2018. Polices and investigating officer started remanding the criminals and nabbed them from Norway and implied heavy fine on the criminals. Children are guided and let them to use the computer under the supervision from the adults henceforth. Unauthorised access needs to be intent to commit that would be facilitate with the commissioning of further offences to be done through this act. Henceforth internet usage is being leveraged with the cloud based system and the data is protected with digital based locker. The hacking of any such information is being monitored through cyber-people or investigating officer rather leaking of data from hacker’s database.

# Conclusion

From the above topic and based on the discussion made so far it is concluded that the research deals with the IT ethics and law of getting the verdict of stealing information of children’s private data across social media platforms. In the modern days, social media usage by every individual, especially children, has grown so much that unintentionally children are falling into cyberbullying scams and threats. Social issues and impacts that would be highlighted are covered in this context of reading children's data gets leaked out. Economic issues and technological impact thus also highlighted had made the context to be proven about children’s safety standards while using social media. Ethical considerations must be also taken into account about the ethics that are being controlled and followed regarding the protection of data.

# Reference List

Data Protection Act 2018, Available at: https://www.legislation.gov.uk/ukpga/2018/12/section/2 (Accessed: 19/03/2023)

Children Act 1989, Available at: https://www.legislation.gov.uk/ukpga/1989/41/section/1 (Accessed: 23/03/2023)

Computer Misuse Act 1990, Available at: https://www.legislation.gov.uk/ukpga/1990/18/section/1#commentary-c19759931 (Accessed: 25/03/2023)

Banet-Weiser, S., 2021. ‘Ruined’lives: Mediated white male victimhood. *European Journal of Cultural Studies*, *24*(1), pp.60-80.

Benyusz, M. and Hulko, G., 2021. Regulation of social media's public law liability in the Visegrad States. *Institutiones Administrationis-J. Admin. Sci.*, *1*, p.6.

Blackwell, L., Ellison, N., Elliott-Deflo, N. and Schwartz, R., 2019. Harassment in social virtual reality: Challenges for platform governance. *Proceedings of the ACM on Human-Computer Interaction*, *3*(CSCW), pp.1-25.

Crocco, M.S., Segall, A., Halvorsen, A.L., Stamm, A. and Jacobsen, R., 2020. “It's not like they're selling your data to dangerous people”: Internet privacy, teens, and (non-) controversial public issues. *The Journal of Social Studies Research*, *44*(1), pp.21-33.

Joshi, D. and Patwardhan, M., 2023. Tracing prodromal behavior by analyzing data patterns from social media with an ensemble machine learning approach. *International Social Science Journal*, *73*(247), pp.29-50.

Obermayer, N., Kővári, E., Leinonen, J., Bak, G. and Valeri, M., 2022. How social media practices shape family business performance: the wine industry case study. *European Management Journal*, *40*(3), pp.360-371.

Richard, C., Karić, M.S., McConnell, M., Poole, J., Rupp, G., Fink, A., Meghdadi, A. and Berka, C., 2021. Elevated inter-brain coherence between subjects with concordant stances during discussion of social issues. *Frontiers in Human Neuroscience*, *15*, p.611886.

Silver, L., Smith, A., Johnson, C., Taylor, K., Jiang, J., Anderson, M. and Rainie, L., 2019. Mobile connectivity in emerging economies. *Pew Research Center*, *7*.

Sufi, F.K., Razzak, I. and Khalil, I., 2022. Tracking Anti-Vax Social Movement Using AI-Based Social Media Monitoring. *IEEE Transactions on Technology and Society*, *3*(4), pp.290-299.

Van Dijck, J., Nieborg, D. and Poell, T., 2019. Reframing platform power. *Internet Policy Review*, *8*(2), pp.1-18.

# Talktalk hack boy admits 7 charges computer misuse (2016), | https://www.ispreview.co.uk/index.php/2016/11/talktalk-hack-boy-admits-7-charges-computer-misuse-act.html