OLUWAFEMI MARK EKE

S4215516

FINTECH

CYBERLAW ASSIGNMENT

BM7214

INTRODUCTION

Cyberlaw is a branch of law that addresses the legal issues related to cyberspace, including cybercrime, data protection, privacy, intellectual property, and electronic commerce. (UNODC, 2013). The rapid changes and challenges presented by new technology and online activities have necessitated a constant evolution of cyber law. One of the crucial subjects in this field is the role and responsibility of platform providers, including social media corporations, cloud service providers, and online marketplaces, in regulating cyber issues. These platform providers hold a significant amount of control and influence over the online environment, as they are responsible for producing, hosting, regulating, and monetizing online content and services. As a result, the question of their accountability in addressing cyber concerns is a key concern in the field of cyber law (Koops et al., 2019). Despite the benefits of platform providers, they encounter several moral and legal dilemmas such as ensuring the accountability of user-generated content, adhering to data protection regulations, safeguarding intellectual property rights, preventing cyberattacks, and upholding human rights (Laidlaw & Young, 2018).

In recent years, there has been a growing debate on whether platform providers should be permitted to self-police their own platforms or whether the law should take a more active role in regulating cyber problems. This conversation involves numerous parties, including governments, regulators, courts, civic society, academics, businesses, and users, each with different perspectives and goals. These viewpoints and objectives range from public interest and consumer protection to innovation, privacy, and competitiveness. (DCMS & Department for Science Innovation & Technology [DSIT], 2022).

The aim of this research is to examine the debate of platform providers being fully responsible for self-policing or the government should shoulder the responsibility. The research will be divided into four sections: regulation, platform providers, evaluation, and recommendation. The first section takes a comprehensive approach by exploring the cyber landscape, including cybercrime related to fraud and child sexual abuse, as well as the laws and regulations surrounding these issues and topics. The second section examines the self-policing mechanisms employed by platform providers to ensure compliance with legal and regulatory requirements. Finally, the third and fourth sections, will be about the evaluation of these mechanisms employed by platform providers, and recommendations will be given based on whether the law should take a more proactive role in regulating cyber matters or if the responsibility should be solely on platform providers. By dividing the research into these sections, a clear and systematic approach is adopted, allowing for a comprehensive analysis of the subject.

REGULATORS

Cyber Crime

n today's digital age, cybercrime has emerged as a major threat due to the prevalence of criminal actions that take place online. According to the 2021 Cybercrime Report by Cybersecurity Ventures, the statistics are alarming, with the cost of cybercrime increasing from $3 trillion in 2015 to a projected $6 trillion globally by 2021. (Cybersecurity Ventures, 2021). The Crime Survey for England and Wales (CSEW) has reported a significant increase in the number of recorded cybercrime incidents in the UK. Specifically, the year ending in March 2021 saw 3.4 million incidents recorded, which is more than double the 1.7 million incidents recorded the previous year (Office for National Statistics, 2021). According to the CSEW, there were 1.7 million cases of computer abuse and 3.7 million incidents of fraud in the year ending March 2021. The most frequent forms of computer abuse were phishing scams (54%), unauthorised access to personal information (28%), and computer viruses or malware (18%). The most frequent forms of fraud were online shopping or auction fraud (29%), advance fee fraud (21%), and consumer or retil fraud (16%) (ONS, 2021). In 2020, IC3 received 791,790 complaints of internet-related crimes, with a total loss of $4.2 billion (IC3, 2020). The most frequent types of internet-related crimes reported to IC3 were extortion scams (15%), non-payment or non-delivery scams (19%), and phishing scams (28%). The necessity for laws and regulations to be proactive in addressing cybercrime is apparent, as cybercrime continues to increase in volume and variety. Cyber fraud and the alarming rise of child sex abuse are just two examples of the many types of cybercrime.

Cyber Fraud

Financial losses, reputational impact, privacy invasion, and even harm to national security are all frequently caused by cyber fraud. To prevent, identify, and criminalise cyber fraud, it is crucial to have strong rules and regulations.

There are various laws in place that aim to prevent cyber fraud across different countries, such as the Fraud Act of 2006, the CFAA, and the CMA. While these regulations offer some benefits, they also have their own set of limitations. Given the constantly evolving and complex nature of cyber fraud, it is possible that these laws may not be sufficient to address the issue effectively.

A UK law known as the Fraud Act of 2006 regulates a variety of fraud offences, including cyber-enabled fraud. The Fraud Act of 2006 has the advantage of being broad and flexible because it simply requires evidence of dishonest intent and doesn't need proof of deception or dishonesty. Many types of internet fraud are covered by the Fraud Act of 2006, which also applies to situations in which someone receives services dishonestly without paying or intending to pay. The Fraud Act of 2006 does, however, have several restrictions, such as the absence of extraterritorial jurisdiction, which precludes its application in situations in which the perpetrator or the victim are located outside of the United Kingdom. Additionally, cyber-dependent fraud that depends on hacking or malware is not covered by the Fraud Act of 2006 and requires a new law [CPS], 2019).

The Computer Fraud and Abuse Act (CFAA) is a US statute that prohibits unauthorized access to a computer or gaining more access than necessary. Since its inception in 1986 as an addition to an existing computer fraud statute, the CFAA has undergone numerous revisions. The statute is advantageous because it is comprehensive and explicitly addresses various types of cyber-dependent frauds, including malware, extortion, phishing, hacking, and denial of service attacks. Furthermore, it has extraterritorial jurisdiction, which allows it to be applied even when the perpetrator or victim is outside of the United States. Despite its strengths, the CFAA has notable flaws, such as the ambiguous and vague terminology used in its provisions regarding authorization and access. Additionally, some criticize the CFAA as being overly broad, resulting in potential misuse or abuse (Goldman, 2013).

The CMA is a UK law that relates to offences or attacks against computer systems such as hacking or denial of service. The CMA was enacted in 1990 as a response to the lack of existing laws to deal with computer misuse. The CMA has the advantage of being simple and clear, as it does not require proof of damage or harm, but only proof of unauthorized access or modification of computer material. The CMA also has extraterritorial jurisdiction, which means that it can apply to cases where the offender or the victim are outside the UK. However, the CMA has some limitations, such as the lack of coverage for cyber-enabled fraud, such as online banking fraud or identity theft (CPS, 2019). The CMA also has been criticized for being outdated and inadequate, as it does not reflect the current technological developments and challenges (Lawyer Monthly, 2020). Moreover, the CMA has been accused of being ineffective and slow in enforcing its powers and imposing sanctions on offenders (Gov.uk, 2021a; 2021b)

Child Sexual Abuse

Child sexual abuse is a grave concern in the digital era as online platforms have created fresh opportunities for perpetrators to exploit children (Europol, 2017). To address this issue, the UK government has implemented several laws and policies such as the Protection of Children Act 1978 and the Sexual Offences Act 2003, which criminalize the possession and distribution of child pornography and other forms of sexual abuse (Home Office, 2021a; 2021b). These laws have been updated in response to evolving online activity, with the Criminal Justice and Courts Act 2015 introducing new offences related to the possession and distribution of "paedophile manuals," and the Serious Crime Act 2015 making it illegal to encourage or request the sexual abuse of a child (Home Office, 2021a; 2021b). Nonetheless, there are still challenges in enforcing these laws and addressing online child sexual abuse (Childnet International, 2021). Other laws aimed at dealing with this cybercrime include the Computer Misuse Act 1990, which prosecutes individuals engaging in online grooming or other forms of online child sexual abuse (Gov.uk, 2021c). Furthermore, the UK government is currently considering the Online Safety Bill, which proposes measures to improve online safety for children, including provisions to prevent children from accessing harmful content and to tackle online child sexual abuse (UK Parliament, 2021).

PLATFORM PROVIDERS

Platform providers are companies that offer online platforms for users to create and share content, communicate, and interact with each other. These platforms include social media sites, video-sharing sites, online marketplaces, and other online services. According to Gillespie (2018), platform providers "are key actors in shaping public discourse and social interaction, and have become powerful brokers in the media landscape" (p. 3). They have a significant influence on the way people access and consume information, communicate with each other, and participate in public discourse. As such, platform providers have a responsibility to ensure that their platforms are safe and compliant with legal and regulatory requirements

One of the main mechanisms that platform providers use is content moderation. While content moderation can help to remove harmful content, there are concerns about the consistency and accuracy of moderation decisions. There have been cases where platforms have removed legitimate content and left harmful content online or have removed content that did not violate their policies. This inconsistency can undermine the trust that users have in the platforms (Gillespie, 2018).

Another mechanism that platform providers use is user reporting. User reporting can help to identify harmful content, but it also raises concerns about abuse and harassment. There have been cases where users have used reporting systems to harass and silence others, or where platforms have removed content simply because it was reported many times, without considering whether it violated their policies (Bruns et al., 2021).

Automated detection tools are another mechanism that platform providers use. While these tools can be effective in detecting harmful content, there are concerns about their accuracy and potential biases. Machine learning algorithms can produce inaccurate or biased results if they are trained on biased data, which can lead to the over- or under-removal of certain types of content (Citron & Norton, 2018).

Finally, there are concerns about the transparency of platform providers' self-policing mechanisms. Many platforms do not provide clear information about how their content moderation or reporting systems work, which can make it difficult for users to understand why their content was removed or how to appeal a decision (Gillespie, 2018).

EVALUATION

* Based on the insights from Gillespie's "Custodians of the Internet" (2018), platform providers have become powerful brokers in the media landscape and play a significant role in shaping public discourse and social interaction. They are responsible for enforcing content moderation policies and practices, which determine what content is allowed or removed on their platforms. An example is a case study on Pornhub accused of hosting child abuse material and monetizing non-consensual videos of sexual violence against children (Paul,2020). The campaigns from small groups, organization and also sanctions from credit firm partners forced Pornhub to self-police in verifying every uploader (Paul, 2020). This is one of the many cases of content moderation. However, there are concerns about the consistency, accuracy, and transparency of moderation decisions. Gillespie, (2018) highlights that the "hidden decisions" made by platform providers have a significant impact on public discourse and raise important questions about the role of regulation and accountability in the digital age. While Gillespie’s analysis of content moderation by platform providers is insightful and provocative, it overlooks some of the benefits and challenges of this practice. Content moderation is not only a matter of enforcing rules and removing harmful or illegal content, but also a way of enhancing user experience, fostering community standards, and promoting diversity and inclusion. Platform providers have to balance competing interests and values, such as freedom of expression, privacy, security, and public interest. They also have to deal with the complexity and ambiguity of online content, which may vary in context, meaning, and intent. Content moderation is not a perfect or neutral process, but it is necessary and inevitable in the digital age. Platform providers should not be seen as custodians of the internet but as partners in a collaborative effort to create a safe and respectful online environment for everyone.
* Content moderation is not the only way that platform providers exert power over the internet. They also gather huge amounts of user data, which can be used for various purposes, such as targeted advertising. This poses privacy and data protection risks. Many users are unaware of how their data is collected, used, and shared by platform providers. It can be sold without their consent or misused. It can be argued that user data is not only a source of power for platform providers but also a valuable resource for innovation and social good. They use user data to improve their services, offer personalized recommendations, and enhance user satisfaction. They also share user data with third parties, such as researchers, policymakers, and civil society organizations, who can use it for various purposes, such as advancing scientific knowledge, informing public debate, and addressing social problems. Platform providers have to comply with data protection laws and regulations, which ensure that user data is collected, used, and shared in a lawful and ethical manner. They also give users control over their data, such as allowing them to access, delete, or modify their data. User data is not a threat to privacy, but an opportunity for progress.
* Another issue with platform providers is their lack of accountability. They often deny responsibility for the content posted by their users, claiming to be neutral intermediaries. However, as Gillespie, (2018) points out, they act as “custodians of the internet” and have significant power over the content that is shared on their platforms. Therefore, they should be accountable for the content moderation decisions they make and the impact they have on public discourse. Though Platform providers are not the only ones who should be accountable for the content posted by their users. They are also subject to the laws and regulations of the countries where they operate, as well as the norms and expectations of their users and stakeholders. They have to cooperate with law enforcement authorities, civil society organizations, and other platforms to address illegal or harmful content. They also have to respect the rights and preferences of their users, such as freedom of expression, privacy, and data protection. Platform providers are not “custodians of the internet”, but participants in a complex and dynamic online ecosystem.

Platform providers have a responsibility to comply with data protection laws and regulations, and to ensure that user data is collected, used, and shared in a lawful and ethical manner. They also have a duty to cooperate with law enforcement authorities, civil society organizations, and other platforms to address illegal or harmful content such as child pornography (child sexual abuse). The government and regulating bodies play a crucial role in overseeing the practices of platform providers and holding them accountable for their actions. By working together in partnership, cyber crimes such as cyber fraud can be mitigated.

RECOMMENDATION

Based on the research so far, it is clear that a partnership between the law and platform providers will derive more improvement and development than the responsibility being solely placed on either the law or platform providers. Here are some recommendations for this proposed collaboration:

Platform providers should provide Accountability by reporting issues or challenges faced with users concerning the laws and regulation in relation to the platform. In terms of content moderation like the removal or fight against child sexual abuse, the platform providers should give comprehensive reports on agreed basis as a show or demonstration of effort in collaborating with the law on content moderation (Gillespie, 2017)

Platform providers handle enormous data collected from users based on the usage of their platform and have tremendous control over this data. This drives towards the importance of user data handling. There should be some form of transparency to the users on their data and how it is being handled due to the unawareness of users on usage of their data, how it is collected and shared by platform providers. One way to improve this transparency is by cutting down on the long user agreement that any educated user reads compared to uneducated users. This contractual user agreement should be innovated upon to improve inclusion in the visibility of transparency. This effort of transparency by platform providers should also be enforced by law, thereby creating a form of collaboration between the law and platform providers.

Due to the absence of technical knowledge and the unforeseen growth of technology, the law will always play a catch-up game in reference to technology, just like the emergence of AI and Chat GPT. Platform providers have the technical knowledge to adjust algorithms to their benefit or fitting in a way the way law will need to catch up to through a case or a follow up crime like many other acts that evolved. Therefore it is recommended that law and platform providers should collaborate to have a proactive approach in stopping cyber crimes such as cyber fraud. This partnership will develop holistic approach of the law in addressing cyber issues.

CONCLUSION

Over time, debates have emerged regarding whether platforms should be self-governed or externally regulated (Gillespie, 2017). While laws and regulations have been established to address these concerns, the law often struggles to keep pace with developments in cyberspace. However, a partnership between platform providers and the law could narrow this gap, fostering a healthy and secure cyberspace that respects and protects all users. Such a collaboration would benefit both platform providers and the law. In conclusion, this study highlights the need for ongoing research into these issues, as the law continues to adapt to modern norms and leave outdated values behind. Future research could explore the complex issues surrounding this study in greater detail.

REFERENCES

1. Action Fraud. (2020). Fraud and cybercrime national statistics.
2. Bruns, A., Enli, G. S., Skogerbø, E., Larsson, A. O., & Christensen, C. (2021). Social media: Usage and impact. Springer.
3. Citron, D. K., & Norton, H. E. (2018). Intermediaries and hate speech: Fostering digital citizenship for our information age. The University of Chicago Law Review, 85, 45-96.
4. Childnet International. (2021). Online child sexual abuse.
5. Crown Prosecution Service. (2019). Cybercrime - prosecution guidance.
6. The Crown Prosecution Service. (n.d.). Computer Misuse Act. Retrieved from <https://www.cps.gov.uk/legal-guidance/computer-misuse-act>
7. Cybersecurity Ventures. (2021). 2021 Cybercrime Report. Retrieved from <https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/>
8. Davies, S. (2019). Obscenity law and the internet. In A. D. Murray (Ed.), The Cambridge Handbook of Copyright in Street Art and Graffiti (pp. 192-211). Cambridge University Press.
9. DCMS & DSIT. (2022). 2022 cyber security incentives and regulation review. https://www.gov.uk/government/publications/2022-cyber-security-incentives-and-regulation-review
10. Europol. (2017). Internet facilitated sexual offending.
11. Gillespie Tarleton. (2017). Regulation of and by platforms. SAGE Handbook of Social Media
12. Gillespie, Tarleton (2018). Custodians of the internet: Platforms, content moderation, and the Hidden Decisions That Shape Social Media. Yale University Press.
13. Glover, S. (2013). The Civic Government (Scotland) Act 1982: its place in the history of Scottish licensing law. Journal of the Law Society of Scotland, 58(6), 7-10.
14. Goldman, E. (2013). The Computer Fraud and Abuse Act is a failed experiment. Forbes. https://www.forbes.com/sites/ericgoldman/2013/03/28/the-computer-fraud-and-abuse-act-is-a-failed-experiment/
15. Gov.uk. (2021a). Investigation into Apple AppStore.
16. Gov.uk. (2021b). Social media endorsements
17. Gov.uk. (2021c). Computer Misuse Act 1990.
18. Greenfield, S., Osborn, G., & Robson, P. (2019). The Civic Government (Scotland) Act 1982 and the challenge to artistic freedom. Edinburgh Law Review, 23(1), 69-92. doi:10.3366/elr.2019.0548
19. Holt, T. J., & Bossler, A. M. (2016). Cybercrime in progress: Theory and prevention of technology-enabled offenses. Routledge.
20. Home Office. (2021a). Protecting children from sexual exploitation and abuse.
21. Home Office. (2021b). Sexual offences.
22. IC3. (2020). 2020 internet crime report. https://www.ic3.gov/Media/PDF/AnnualReport/2020\_IC3Report.pdf
23. iPleaders. (2020). Cyber crime laws in India. https://blog.ipleaders.in/cyber-crime-laws-in-india/
24. Koops B.-J., Newell B.C., Timan T., Škorvánek I., Chokrevski T., & Galič M. (2019). A typology of privacy. University of Pennsylvania Journal of International Law 40(2), 483-575.
25. Laidlaw E.B., & Young L. (2018). Platform regulation: Restoring trust in social media? Journal of Law Technology & Policy 2018(1), 1-34.
26. Legislation.gov.uk. (2006). Fraud Act 2006. https://www.legislation.gov.uk/ukpga/2006/35/contents
27. Nationwide. (n.d.). Scams guide.
28. Office for National Statistics. (2021). Crime in England and Wales: year ending March 2021. Retrieved from <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2021>
29. ONS. (2021). Crime in England and Wales: Year ending March 2021. <https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2021>
30. Paul, K. (2020, December 14). Pornhub purge removes unverified videos amid investigation into child abuse. The Guardian. <https://www.theguardian.com/technology/2020/dec/14/pornhub-purge-removes-unverified-videos-investigation-child-abuse>.
31. Reid, C. (2014). The Civic Government (Scotland) Act 1982: A critical analysis. Scottish Justice Matters, 2(3), 22-23.
32. Santander UK. (n.d.). Spotting fraud and scams.
33. The National Archives. (n.d.). Obscene Publications Act 1959. <https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66>
34. Wilson, A. (2019). Free speech should not be based on the majority’s morals. The Guardian.
35. UK Parliament. (2021). Online Safety Bill. <https://publications.parliament.uk/pa/bills/cbill/58-01/0268/cbill_2019-20210268_en_1.htm>
36. UNODC. (2013). Comprehensive study on cybercrime. <https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf>