Impact of Cyber Crime on Anonymity, Privacy and Security

Amita Rani Mahato[a] Dr Dipti Kumari[a]

[a] Department of Computer Science Engineering RKDF University, Ranchi

[a] PhD Research Scholar, Department of Computer Science Engineering, RKDF University, Ranchi

Corresponding author email id: amitarani308@gmail.com

ABSTRACT

Anonymity, often considered a cornerstone of democracy and a First Amendment guarantee, is easier to attain than ever before, due to the emergence of cyberspace. Cyberspace enables people to share ideas over great distances and engage in the creation of an entirely new, diverse, and chaotic democracy, free from geographic and physical constraints. As of September 30, 2009, about 1,733,993,741 users had access to the internet. Those numbers are growing rapidly. Due to the nature of ICTs, identities in cyberspace are easily cloaked in anonymity. Once a message sender's identity is anonymous, cyberspace provides the means to perpetrate widespread criminal activity among the masses, with little chance of being apprehended. In a report to former Vice President Al Gore, Attorney General Reno found a need for greater control of anonymity in cybercrime. Reacting to several attacks on eBAY, CNN.com and other websites, former President Clinton underscored the opinion that the government needs to maintain a watchful eye on cyberspace. On the other hand, anonymity in cyberspace allows whistle-blowers and political activists to express opinions critical of employers and the government, enables entrepreneurs to acquire and share technical information without alerting their competitors, and permits individuals to express their views online without fear of reprisals and public hostility. In various parts of the world, people may have an interest in not being identified and thus connected to certain published views and opinions. Due to the international character of the internet, those reasons for anonymous communications which are related to the "freedom of expression" may gain new dimensions.

1. Introduction

1.1 Anonymity in Cyberspace

There are two kinds of anonymity: true anonymity and pseudo-anonymity. However ,some scholars fail to sufficiently address this distinction. Dialogue on the issue of anonymity legislation suffers on account of this lack of distinction. This section will therefore distinguish between true and pseudo—anonymity, two completely different forms of expression, with differing degrees of political and social value and constitutional protection.

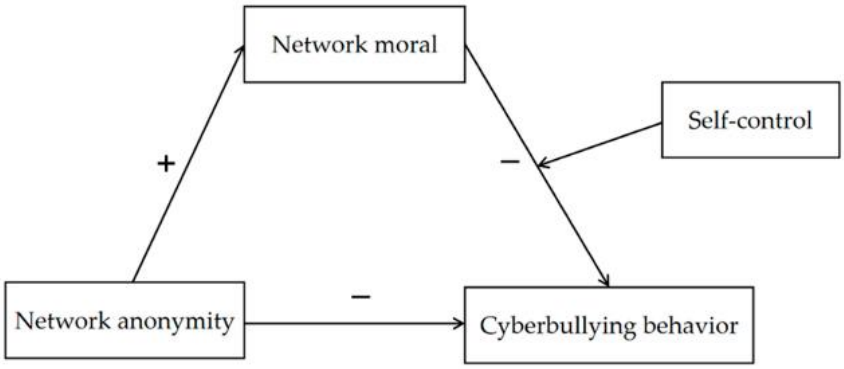

Fig. 1.1 Network Chart

1.2 True Anonymity

Truly anonymous communication is untraceable. Indeed, only coincidence or purposeful self-exposure will bring the identity of the mystery sender to others; the identity of a person acting in a truly anonymous manner cannot be definitively discovered with any amount of diligence. Attempts can be made to discover the identity of the sender through inference, but any concrete trail of clues betraying the message sender has been erased by circumstance, the passage of time, or by the sender herself. Although some forms of truly anonymous communication, such as political speech, are considered valuable, this form of anonymity has exceptional potential for abuse because the message senders cannot be held accountable for their actions.

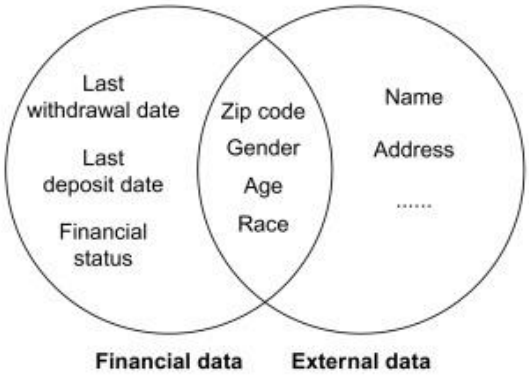

Fig. 1.2 Financial and External Data

1.3 Pseudo-Anonymity

Pseudo-anonymous communication is inherently traceable. Though the identity of the pseudo-anonymous message sender may seem truly anonymous because it is not easily uncovered or made readily available by definition, it is possible to discover their identity. This kind of anonymity has significant social benefits; it enables citizens of a democracy to voice their opinions without fear of retaliation against their personal reputations, but it forces them to take ultimate responsibility for their actions, should the need somehow arise. Although governments could abuse their ability to uncover the identity of people acting pseudo—anonymously, it is not in the government's interest to break that trust; by respecting pseudo-anonymous identities, governments can often avoid the far more dangerous abuses stemming from true anonymity.

	Public Blockchain	Private Blockchain	Consortium/Federated Blockchain
Participation in Consensus	every node	Solo organization	Some specified nodes in multiple organizations
Access	Read/write access allowed to all	High access restriction	Comparatively lower access restriction
Identity	Pseudo-anonymous	Accepted participants	Accepted participants
Immutability	Fully immutable	Partially immutable	Partially immutable

Table 1: Blockchain Technology

1.4 Anonymity, Privacy and Freedom of Speech

The world in which we live can frequently be extremely conservative, often making it dangerous to make certain statements, have certain opinions, or adopt a certain lifestyle. Anonymity is important for online discussions involving sexual abuse, minority issues, harassment, sex lives, and many other things. Moreover, anonymity is useful for people who want to ask technical questions that they do not want to admit they do not know the answer to, report illegal activities without fear of retribution, and many other things. Without anonymity, these actions can result in public ridicule or censure, physical injury, loss of employment or status, and in some cases, even legal action. Protection from harm resulting from this type of social intolerance is a definite example of an important and legitimate use of anonymity on the internet.

2. Result and Discussion

The results of earlier investigations and records make it clear that as technology develops, cybercrime likewise rises. The startling reality that more competent individuals commit cybercrimes encourages everyone to learn about the fundamental rules and ethics of internet usage. Undoubtedly, cybercrime and hacking present a significant risk to secure internet use. This can make use of a variety of methods and instances from prior incidents to somewhat lessen cybercrime. To effectively control cybercrime, strict cyber laws must also adapt and evolve at the same rate as hackers. Therefore, there should be a balance between safeguarding citizens' rights and preventing crime. The main benefits of the internet are its size and accessibility for free. However, the issue of whether it can take decisive action against cybercriminals comes up. It has been observed that as security is tightened, intruders move forward. Cybercriminals and cyber terrorists will face many unforeseen difficulties that can be avoided with a tight and constructive partnership and participation of both the individual and the government. The goal is to concentrate on creating a trustworthy, secure, and safe computing environment for everyone. Without a doubt, it is essential to maintain both our economy and our security. The Indian government has occupied a number of measures to reduce cybercrimes and promote safe internet use, but cyber legislation cannot remain static. It should be properly modified with the development of time and technology.

3. Conclusion

This paper outlines the significance of cybercrime for communication technology and information and gives the theoretical underpinnings for the components in the current research project. According to various research, internet cyber laws have been implemented to safeguard users. While the majority of cybercrimes are committed to making money for the perpetrators, some are committed against specific systems or devices to harm or disable them. The sensitive data is at risk from cyber attacks that are becoming more complex and dynamic as hackers use innovative techniques fuelled by Social Engineering and Artificial Intelligence (AI) to get around established data protection measures. The reliance on technology around the globe is increasing and this dependence will only increase as we

develop the new technologies that will link to our connected devices via Bluetooth and Wi-Fi in the future. The researcher will analyse numerous case studies involving cybercrime using software tools in the next paper. This rapidly explains that specific technological know-how and equipment are necessary for conducting cybercrime investigation and prevention strategies.

4. Acknowledgement

The first author would like to acknowledge the fellowship support from RKDF Unvesity, Ranchi India which enabled her to accomplish the study wth her guide(2nd author). The authors are indebted to the IUCN, India for providing the financial support to conduct the field investigations. The authors would like to express their gratitude to Jamshedpur Cyber Police Station.

References

1. *Alagarsamy, S., Selvaraj, K., Govindaraj, V., Kumar, A.A., HariShankar, S. and Narasimman, G.L., (2021), September. Automated Data analytics approach for examining the background economy of Cybercrime. In 2021 Third International Conference on Inventive Research in Computing Applications (ICIRCA) (332-336). IEEE.*
2. *Sameera, K. and Vishwakarma, P., (2019). Cybercrime: To Detect Suspected User's Chat Using Text Mining. In Information and Communication Technology for Intelligent Systems (381-390). Springer, Singapore.*
3. *Dremliuga, R., Dremliuga, O. and Kuznetsov, P., (2020). Combating the Threats of Cybercrimes in Russia: Evolution of the Cybercrime Laws and Social Concern. Communist and post-communist studies, 53(3), 123-136.*
4. *Mngadi, W.B., (2021). An analysis of cybercrime investigation by Directorate for Priority Crime investigation (Doctoral dissertation).*
5. *Nyman Gibson Miralis, (2020), https://www.lexology.com/library/detail.aspx?g=12513d17-cff3-4d8f-b7dc-cd91826f05d4*
6. *Dmitrieva, K.N. and Mishina, N.O., (2022). Cybercrime–the Weapon of Mass Destruction, 2022, pp.25-30.*
7. *Caneppele, S. and Aebi, M.F., (2019). Crime drop or police recording flop? On the relationship between the decrease of offline crime and the increase of online and hybrid crimes. Policing: A Journal of Policy and Practice, 13(1), pp.66-79.*
8. *Farrand, B. and Carrapico, H., (2021). The How and Why of Cybercrime: The EU as a Case Study of the Role of Ideas, Interests, and Institutions as Drivers of a Security-Governance Approach. In Researching Cybercrimes (pp.23-41).Palgrave Macmillan, Cham.*
9. *Motlhabi, M., Pantsi, P., Mangoale, B., Netshiya, R. and Chishiri, S., (2022), March. Context-Awar Cyber Threat Intelligence ExchangePlatform In International Conference on Cyber Warfare and Security (Vol. 17, No. 1, pp. 201-210).*
10. *Alese, T., Owolafe, O., Thompson, A.F. and Alese, B.K., (2021). A User Identity Management System for Cybercrime Control. Nigerian Journal of Technology, 40(1), pp.129-139.*
11. *Ghazi-Tehrani, A.K. and Pontell, H.N., (2021).Phishing evolves: Analyzing the enduring cybercrime. Victims & Offenders, 16(3), pp.316-342.*
12. *Richardson, W., Butt, U.J. and Abbod, M., (2021). Critical Review of Cyber Warfare Against Industrial Control Systems. Information Security Technologies for Controlling Pandemics, pp.415-434.*
13. *Cascavilla, G., Tamburri, D.A. and Van Den Heuvel, W.J., (2021). Cybercrime threat intelligence: Asystematic multi-vocal literature review. Computers &Security, 105, p.102258.*
14. *Bouwman, X., Le Pochat, V., Foremski, P., Van Goethem, T., Gañán, C.H., Moura, G., Tajalizadehkhoob, S., Joosen, W. and van Eeten, M., (2022). Helping hands: Measuring the impact of a large threat intelligence sharing community. In Proceedings of the 31st USENIX Security Symposium. USENIX Association.*
15. *Shanti, D., (2020). A New State of Organized Crime: An Analysis of Cybercrime Networks, Activities, and Emerging Threats. The Journal of Intelligence, Conflict, and Warfare, 3(1), pp.13-13.*
16. *Di Nicola, A., (2022). Towards digital organized crime and digital sociology of organized crime. Trends in Organized Crime, pp.1-20.*
17. *Shandler, R., Gross, M.L., Backhaus, S. and Canetti, D., 2022. Cyber terrorism and public support for retaliation–a multi-country survey experiment. British Journal of Political Science, 52(2), pp.850-868.*

18. *Willing, M., Dresen, C., Haverkamp, U. and Schinzel, S., (2020). Analyzing medical device connectivity and its effect on cyber security in german hospitals. BMC medical informatics and decision making, 20(1), pp.1-15.*
19. *Backhaus, S., Gross, M.L., Waismel-Manor, I., Cohen, H. and Canetti, D., (2020). A cyberterrorism effect? Emotional reactions to lethal attacks on critical infrastructure. Cyberpsychology,Behavior, andSocialNetworking, 23(9), pp.595-603.*
20. *Stalans, L.J., (2022), May. Social and Emotional Context of Fraud Scams in Cyberspace. In Proceedings of the 1st Workshop on Cybersecurity and Social Sciences (pp. 1-1).*
21. *Chawla, A., Yu, J. and Ng, S., (2021). Cybercrime and scams amidst COVID-19: A review of the human vulnerabilities exploited during a global pandemic. Introduction to cyber forensic psychology: Understanding the mind of the cyber deviant perpetrators, 205-227.*
22. *Custers, B., Oerlemans, J.J. and Pool, R., (2020). Laundering the profits of ransomware: Money laundering methods forvouchersandcryptocurrencies. European Journal of Crime, Criminal Law and Criminal Justice, 28(2), pp.121-152.*
23. *Gilmour, P.M., (2022). Re-examining the anti-money-laundering framework: a legal critique and new approach to combating money laundering. Journal of Financial Crime.*
24. *Buchanan, B., (2020). The hacker and the state: Cyber attacks and the new normal of geopolitics. Harvard University Press.*
25. *Lee, K.B. and Lim, J.I., (2016). The Reality and Response of Cyber Threats to Critical Infrastructure: A Case Study of the Cyber-terror Attack on the Korea Hydro & Nuclear Power Co., Ltd. KSII Transactions on Internet and Information Systems (TIIS), 10(2),857-880.*
26. *Wang, S.Y.K., Hsieh, M.L., Chang, C.K.M., Jiang, P.S. and Dallier, D.J., (2021). Collaboration between law enforcement agencies in combating cybercrime: Implications of a Taiwanese case study aboutATMHacking. International journal of offender therapy and comparative criminology, 65(4), 390-408.*
27. *Brierley, C., Arief, B., Barnes, D. and Hernandez-Castro, J., (2021), November. Industrialising Blackmail: Privacy Invasion Based IoT Ransomware. In Nordic Conference on Secure IT Systems (pp. 72-92). Springer, Cham.*
28. *Rogers, M.K., Seigfried-Spellar, K.C., Bates, S. and Rux, K., (2021). Online child pornography offender risk assessment using digital forensic artifacts: The need for a hybrid model. Journal of forensic sciences, 66(6),.2354-2361.*
29. *Andrade, M., Sharman, S., Xiao, L.Y. and Newall, P., (2022). Safer gambling and consumer protection failings amongst 40 frequently visited cryptocurrency- based online gambling operators.*
30. *van der Maas, M., Cho, S.R. and Nower, L., (2022). Problem gambling message board activity and the legalization of sports betting in the US: A mixed methods approach. Computers in Human Behavior, 128, 107133.*
31. *Wardle, H., Reith, G., Dobbie, F., Rintoul, A. and Shiffman, J., (2021). Regulatory resistance? Narratives and uses of evidence around "black market" provision of gambling during the British gambling act review. International journal of environmental research and public health, 18(21), 11566.*
32. *Gumelar, A.B., Adi, D.P., Setiawan, E., Widodo, A. and Sulistyono, M.T., (2020), September. Machine Learning Performance Comparison for Toxic Speech Classification: Online Payday Loan Scams in Indonesia. In 2020 International Seminar on Application for Technology of InformationandCommunication (iSemantic) (pp. 603-608). IEEE.*
33. *Maghfirah, F. and Husna, F., (2021). Cyber crime and privacy right violation cases of online loans in indonesia. In PROCEEDINGS: Dirundeng International Conference on Islamic Studies, 1-18.*
34. *Sauerwein, C., Sillaber, C. and Breu, R., (2018). Shadow cyber threat intelligence and its use in information security and risk management processes. Multikonferenz Wirtschaftsinformatik (MKWI 2018), pp.1333-1344.*
35. *Perkins, R.C. and Howell, C.J., (2021). Honeypots for cybercrime research. In Researching Cybercrimes (pp. 233-261). Palgrave Macmillan, Cham.*
36. *Atefeh, K.S., (2021). The role of fingerprint in scientific crime detection. Фундаментальные и прикладныеисследования в современном мире, (29-2), 174-177.*
37. *Schneider, S. and Kokshagina, O., (2021). Digital transformation: What we have learned (thus far) and what is next. Creativity and innovation management, 30(2), 384-411.*
38. *Jamil, H., Zia, T. and Nayeem, T., (2021). User Acceptance of Password Manager Software: Evidence from Australian Microbusinesses. Journal of Information Security and Cybercrimes Research, 4(2),148-159.*

39. *Younis, Z.K. and Mahmood, B., (2020), February. Towards the Impact of Security Vunnerabilities in Software Design: A Complex Network-Based Approach. In 2020 6th International Engineering Conference "Sustainable Technology and Development"(IEC) (pp. 157-162). IEEE.*
40. *von Solms, S. and Meyer, J., (2021). Use of low bandwidth network technologies and sensors for operation and performance monitoring of rural development projects: A case study in South Africa. The Electronic Journal of Information Systems in Developing Countries, 87(5), p.e12182.*
41. *Chebotareva, A.A. and Chebotarev, V.E., (2021), March. Hardware, Biometric and Passwordless Authentication: Vulnerability and Cybercrime Issues. In IOP Conference Series: Materials Science and Engineering (Vol. 1069, No. 1, p. 012038). IOP Publishing.*
42. *Sherimmatovich, A.E., Atabekovich, B.F. and Farhodovich, B.B., (2022). Implement biometric authentication of users enhancement model and algorithm research. Eurasian Research Bulletin, 6,86-88.*
43. *Bhushan, B. and Saxena, S., (2020). The Dark Web: A Dive Into the Darkest Side of the Internet.*
44. *Giri, S., (2019). Cyber crime, cyber threat, cyber security strategies and cyber law in Nepal. Pramana Research Journal, 9(3), 662-672.*
45. *Altarturi, H.H., Saadoon, M. and Anuar, N.B., (2020). Cyber parental control: A bibliometric study. Children and Youth Services Review, 116, .105134.*

Received 17 September 2024
Revised 12 December 2024
Accepted 17 January 2024