THE INDIAN JOURNAL OF CRIMINOLOGY & CRIMINALISTICS

IJCC
Volume: 1, Issue: 2
December 2025
E-ISSN: 3139-7778

EXPLOITATION OF APP ECOSYSTEM FOR CYBER CRIME

Dr. Sandeep Mittal, IPS

Additional Director General of Police
Cyber Crime Wing, Tamil Nadu Police,
Chennai, Tamil Nadu

INTRODUCTION

Application ecosystem in Cyberspace involves multiplicity of platforms like Web, Android and iOS, etc. Cybercrime is a pervasive and costly global issue. As estimated by a report the cybercrime loss in 2023 is estimated to be 8 trillion USD. Earlier, main mediums that facilitated cybercrimes included phishing emails, fake websites, targeted advertisements, etc., but with the advent of Web 3 technologies, the Mobile Apps are extensively involved in cybercrimes. Earlier, malicious Apps (i.e., malwares such as Back Door and Trojan) that compromised victims' devices and Apps leading to privacy leakage and abuse were prevalent and were mainly used to launch interpersonal attacks rather than to make profits. Recently the Application Ecosystem has evolved into attacking for profit from victims directly through deceiving, threatening or other criminal acts rather than compromising victims' devices. The main platform for developing, deploying and exploiting these Apps is Android Platform. As of early 2024, there are approximately 3.9 billon Android users in the world with a market share of around 71%. While in USA, the iOS holds about 61% of market share, the Android Platform holds about 96% of the mobile operating system market in India. The Android Platform remains a favourite platform for exploitation of App Ecosystem for the cyber criminals for targeting Indian population. The scope of this essay is to identify and discuss the recent trends in exploitation of Android Application Ecosystem and to find a way forward to minimise the impact of these weaponised Apps on Indian users.

METHODOLOGY

To develop this concept paper the scholarly research done all over the world was searched and the references listed in the References Section of the essay were studied. As the time frame for the study was a limitation, the main method for crystallising the ideas was literature review of available research blended with experience of the author in handling Cyberspace. While all malicious Applications in the ecosystem are potential risk, in this essay we would limit our discussion to 'Malware', 'Culpritware', 'Fleeceware' and 'Decentralised Applications' and related issues in view of the emerging potential of these Applications.

PROLOGUE

Before we start our discussion, it would be helpful to understand about some emerging Applications mentioned above. 'Malware' is an application which has uses available technology, is anti-virus proof, has stealth, withstand this disinfection techniques, communicates with Command Centre, extract data stealthily to Control Centre and evades forensic investigation, e.g., 'Stuxnet', 'Duqu', 'Flame', 'Mask' or 'Careto', 'Bad Bios', 'Heart Bleed' and many more. Applications which directly make profit from victims through deceiving, threatening or other criminal action are termed as 'Culpritware' (Zhuo Chen, et al., 2021) and their characteristics and ecosystem remains mysterious. The malicious subscription Apps that trick users into expensive subscriptions leading to substantial financial consequences are termed as 'Fleeceware' (Chang Yue, Chen Zhong, Kai Chen, Zhiyu Zhang, & Yeonjoon Lee, 1999). 'DApps' are the decentralised Apps which do not have a centralised server and impede the establishment of connections between digital accounts and real-world connectivity thus offering anonymity (Arjun Chetry & Uzzal Sharma, 2023). Having understood the definition of these unique Apps, the essay would discuss these in detail in the following paragraphs.

MALWARE

Android malware applications can be downloaded from Google Play Store and from Chinese markets. Chinese markets (e.g. Baidu, Tencent), Lenovo and Huawei studies indicate that Chinese at markets perform substantially worse when taking active measures to protect mobile users and legit developers from deceptive and abusive actors, showing a significantly higher preference of malware, fake and cloned Apps, then Google Play as indicated in figure 1 (Haoyu Wang, et al., 2018).

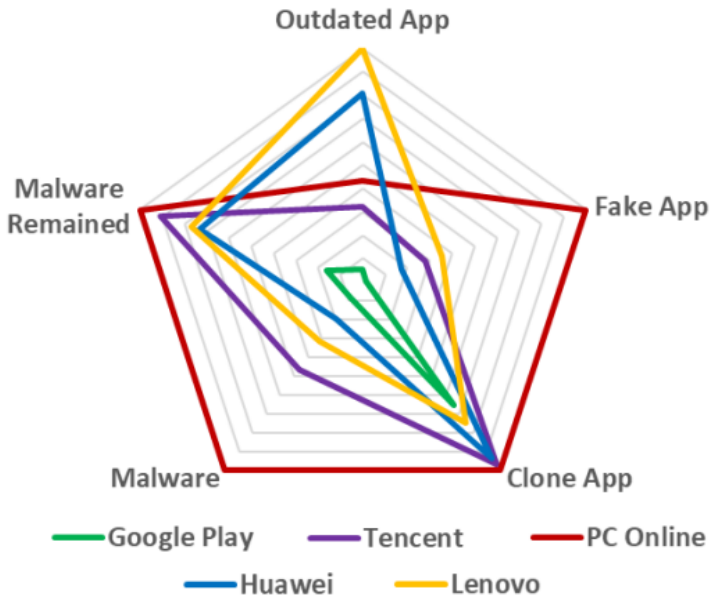


Figure 1: Multi-dimensional comparison of Google Play, Tencent, PC Online, Huawei and Lenovo markets. For each metric, we normalise it to the scale [0,100], and the centre represents 0.

The commercial anti-virus engines and the widely used techniques failed to identify malware as Android malware is evolving all the time and the malware in the new era are greatly different from the old ones posing more challenges. Only 24% of malware were flagged by over 30 engines (Liu Wang, et al., 2022). The malwares are distributed through various distribution channels (Liu Wang, et al., 2022) as indicated in figure 2.

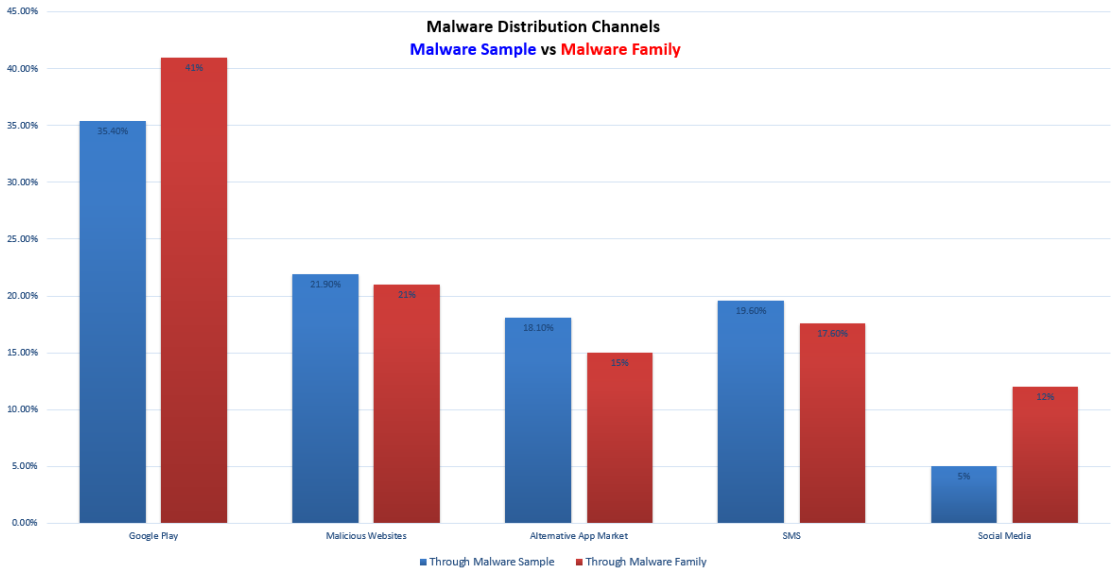


Figure 2: Malware Distribution Channels

As indicated in the figure 2 a large number of malwares were distributed beyond Google Play and third-party markets. These are overlooked by the research community thus making it difficult to regulate. Researchers and regulators should pay more attention to App release channels beyond App markets.

It is interesting to note the evolution of App installation. The techniques of malware installation include, App repackaging, update attack, drive by download, third party library and standalone. Out of these the standalone malware has become the most mainstream way to create the malicious Apps also it is noticed

that malware developers are injecting the malicious payload into third party libraries and load them at run time. System event-based activation ('boot completed' and 'network') remain the main trick to activate the malicious payload. The malicious behaviours of the Android malware have become diverse with Privacy Stealing, Remote Control and Privileged Escalation remaining as most popular behaviours. A number of new emerging activities (e.g., ransomware, mining and premium services subscription) are becoming rampant. 96% of malware uses atleast one anti-analysis technique. Environment check, obfuscation and communicate encryption are the most widely techniques used to evade detection (Liu Wang, et al., 2022). In a study it was found that 14% and 4% of malicious and benign samples refrain from running in an analysis environment that does not correctly mitigate evasive techniques. It would be interesting to understand the evolution of malware from decade ending the year 2010 versus year 2020. The malware has undergone marked evolution over the decade as indicated in figure 3.

Malware Characteristics	Year (2010-2011)	Year (2020-2021)
1 Installation	App Repackaging (84%)	Stand Alone Apps (41%)
2 Activation	Boot Completed Event (83%)	Boot Completed Event(77%)
3 Malicious Behaviour	Remote Control (93%) Privacy Stealing (59%)	Remote Control (85%) Privacy Stealing(90%)
4 Anti-Analysis Techniques	Obfuscation (19%) Encryption (14%)	Obfuscation (96%) Encryption (24%)

Figure 3: Malware Evolution over the decades

Culpritware

'Culpritware' and its ecosystem has unique features making them significantly different from benign Apps and malware. Compared with benign Apps and malware, Culpritware's developers tend to develop hybrid Apps, and abuse 'Apps generators' to facilitate the development. Culpritware use more permissions than the benign Apps while less permission than the Malware Apps. The provenance of Culpritware developers is largely unknown/hidden. Majority of culpritware (52%) are propagated through social media rather than the formal Apps market. The access code is widely used in culpritware and users are converted to an accomplisher through the invitation process. 96% of culpritware adapt covert fourth party payment services indirectly using third party payments by requiring the users to finalise the payments. The Culpritware need closer attention of cyber security community and Law Enforcement Authorities to mitigate the threats (Zhuo Chen, et al., 2021)

Fleeceware

Fleeceware is a type of subscription App that deceives users into incurring unclear or hidden charges. Users may subscribe to Apps without their consent, fail to realise they will be charged after a free trial or struggle to cancel a subscription. Avast reported that in 2021, 204 Fleeceware Apps have brought in 403.5 million USD in revenue (Chang Yue, Chen Zhong, Kai Chen, Zhiyu Zhang, & Yeonjoon Lee, 1999). Majority of the machine learning based methods to detect new types of malwares are ineffective at detecting fleeceware as fleeceware mainly utilises hidden or contradictory content on the user interface to confuse the users and exhibit coding patterns that closely resemble legitimate Apps without resorting to traditional malicious behaviours such as stealing confidential data causing system crashes. Fleeceware uses dark patterns for subscription frauds. Studies have identified several dark patterns, e.g., The interface intentionally hides subscription related information (Sneaking), causing users to unknowingly complete a subscription. The interface prominently highlights the 'free trial' while making the subsequent payment information difficult to notice using small font sizes and inconspicuous colours (interface interference), giving an impression that App will not automatically charge fees. The fleeceware leverages dark patterns to orchestrate subscription App scams leaving to users' financial detriment. These dark patterns should be utilised to identify fleeceware.

THE INDIAN JOURNAL OF CRIMINOLOGY & CRIMINALISTICS
IJCC
Volume: 1, Issue: 2
December 2025
E-ISSN: 3139-7778

Decentralised Apps

Due to the absence of the centralised server and anonymity impeding the establishment of connection between digital accounts and real-world connectivity thus hampering investigation of cybercrimes (Arjun Chetry & Uzzal Sharma, 2023). A bird's eye view of DApps, related frauds and examples is presented in figure 4. There is an urgent need to identify and regulate DApps by multiple technology and policy interventions.

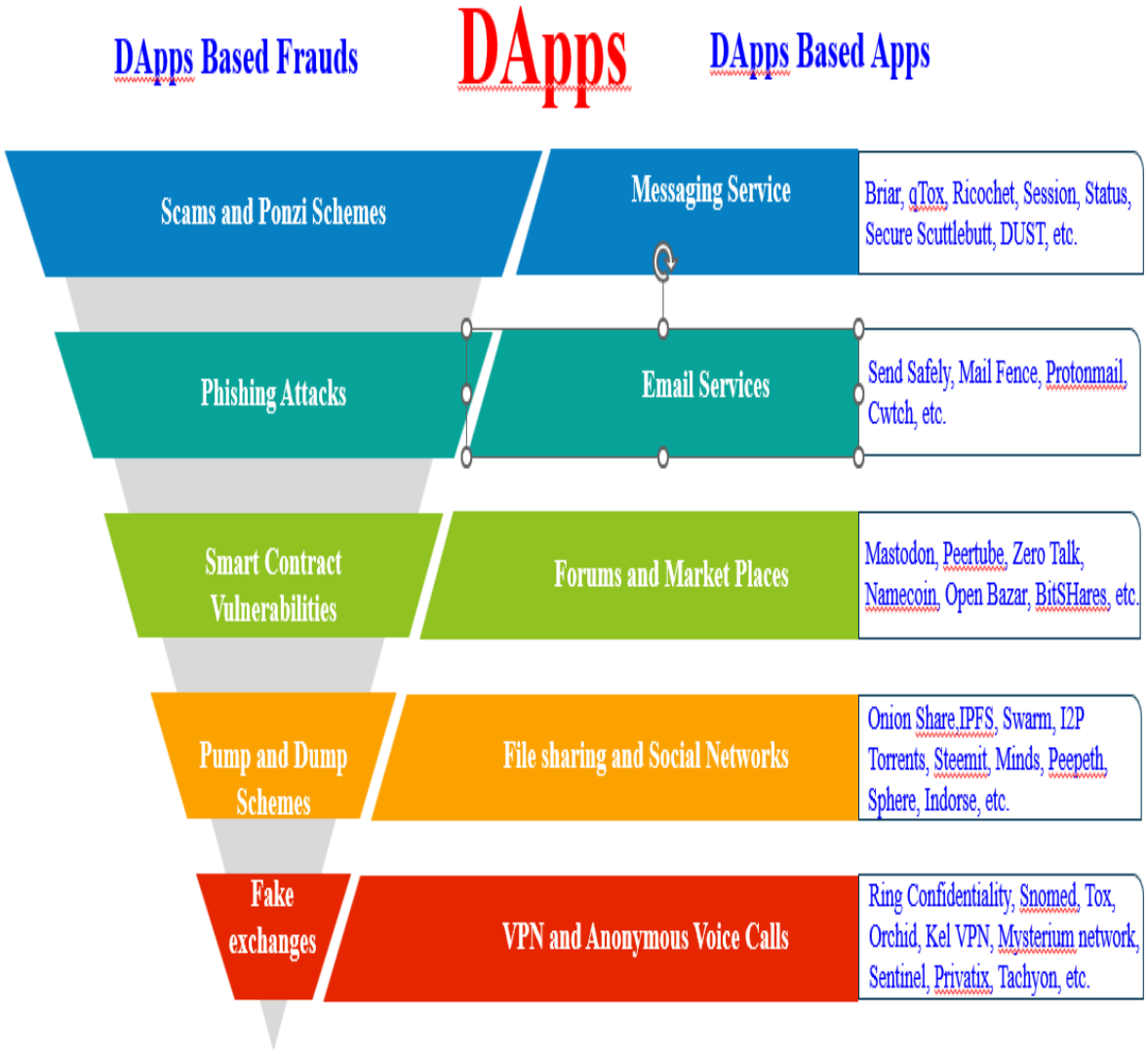


Figure 4: DApps based frauds and list of DApps

We have discussed different emerging App ecosystems viz., Malware, Culpritware, Fleeceware and DApps which are difficult to be identified by normal malware detection engines due to the reasons explained for each. Additionally, the following issues deserves close attention in understanding App ecosystem,

a) 'App Virtualisation' using proxy layer between plug-in Apps and the Android frameworks and loading plug-in stealthily hiding malicious behaviour (Luman Shi, et al., 2020);

b) 'Accessibility Services' utilisation by Apps through online social media (e.g., Twitter, Facebook, Instagram, etc). It has been found that accessibility services users rate for Apps distributed on Google Play was reported to be 0.37% but it was 9.4% for the Apps collected from Twitter (now X) (Shuichi Ichioka, Estelle Pouget, Takao Mimura, Jun Nakajima, & Toshihiro Yamauchi, 2020). The percentages of malwares and benign Apps using Accessibility Services are quite similar posing a challenge in identifying this issue as regard to Apps' malicious behaviour.

c) 'Cryptojacking malware ecosystem' in the Android environment is a serious factor to consider. These mining Apps covertly tend to be embedded into free versions of premium Apps or pose as utility Apps that provide valuable services to users and are distributed through reputed stores like Google Play Store trusted by almost 70% of the google users.

THE INDIAN JOURNAL OF CRIMINOLOGY & CRIMINALISTICS
IJCC
Volume: 1, Issue: 2
December 2025
E-ISSN: 3139-7778

The Way Forward

Having discussed the Application Ecosystem, it would be interesting to see how the App Ecosystem fits into gambit of Cyberspace in the light of Rumsfeld Matrix (theuncertaintyproject, 2002) as depicted in figure 5.

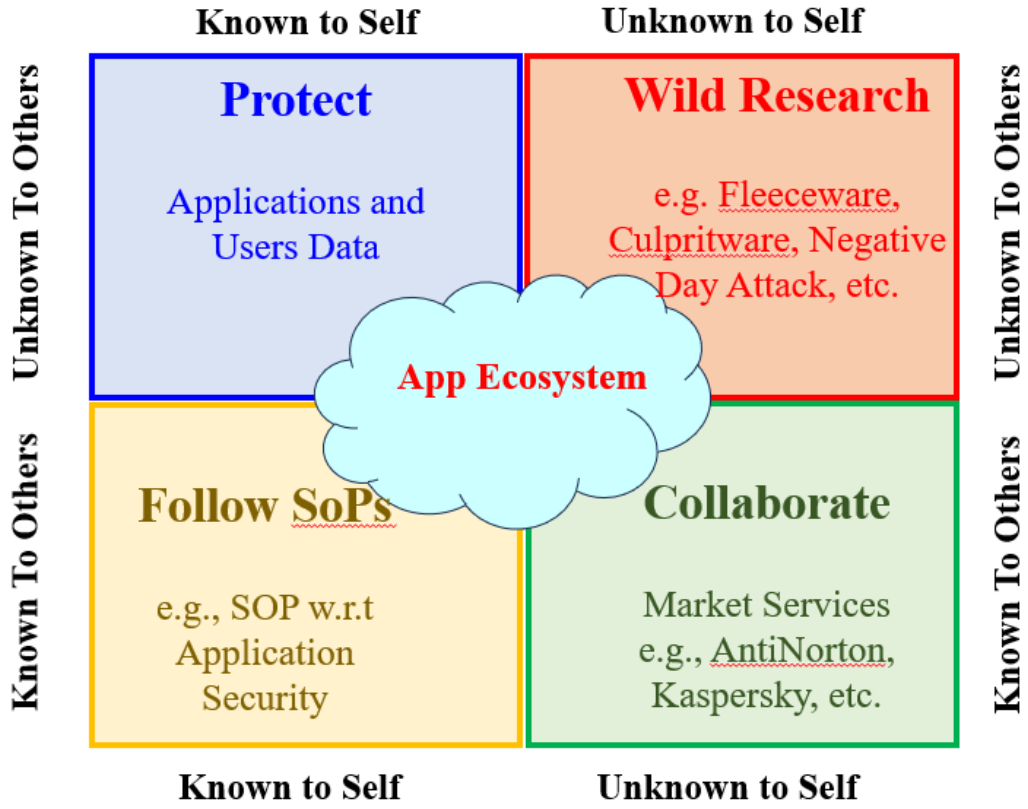
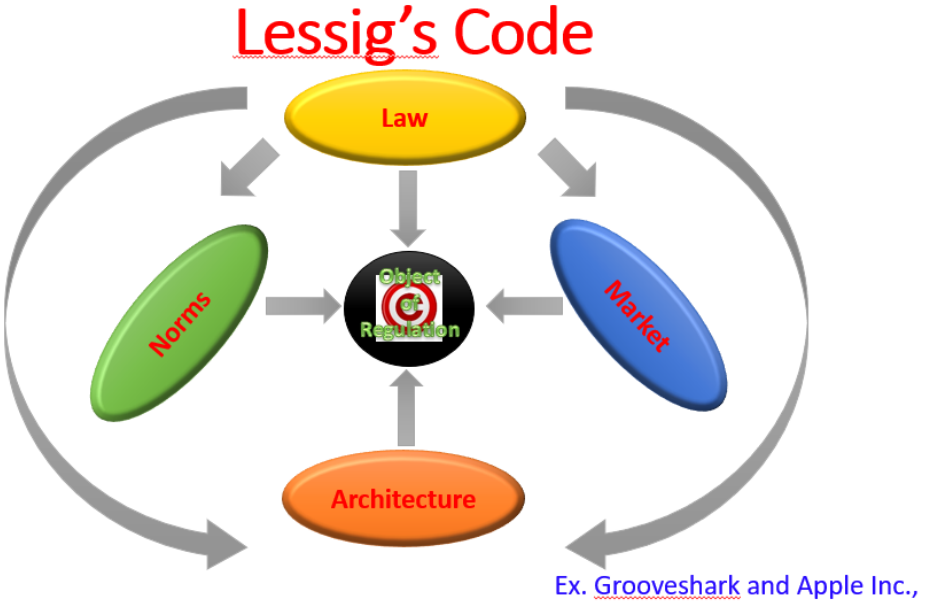


Figure 5: Rumsfeld Matrix

As App Ecosystem is dynamically evolving in space and time, Lessig's code outlines how Law, Architecture, Norms and Markets can be utilised to regulate Cyberspace and implicitly application ecosystem being part of the larger Cyberspace as depicted in figure 6 (Surisetti, 2017)



Modified after Free Culture by Lessig, L., Available at http://libreria.sourceforge.net/library/Free_Culture/CHAPTER10.html

Figure 6: Lessig's Code

We can apply these four modalities to different regulatory issues about Cyberspace. To understand further, let us presume that we are concerned with offensive content hosted on Cyberspace. We could create Law against it but it would be hard to enforce as content is mostly hosted in foreign jurisdiction. A multi-pronged strategy would be desirable to minimise the exploitation of App Ecosystem depending upon the factors affecting the ecosystem. A few such concerns are listed below:

a) Aspects of the App Ecosystem known to us and also to others in Cyberspace need to be monitored and kept sanitised by following Standard Operating Procedures regarding Application Security.

b) Aspects of the App Ecosystem which are known to others but unknown to us (e.g., data sets and research held by malware researchers) need collaboration with market services.

c) Aspects of the App Ecosystem known to us but unknown to others need to be protected pro-actively (e.g., Application and User data, etc.)

d) Aspects of the App Ecosystem unknown to us and others are a cause of concern and need research in the wild (e.g., negative day research is important in this direction).

To regulate these technological aspects of Application Ecosystem the following is suggested,

a) A centralised consortium of academia, researchers and other stakeholders be created to conduct targeted research on various aspects of Application Ecosystem as listed in the above discussion on malware, culpritware, fleeceware, DApps, etc. The funding for designing test bed and reverse malware forensics etc. be provided to the consortium. The consortium would actively identify malicious Apps and create a malware library for sharing with a regulatory body.

b) A regulatory body be created who on receipt of malicious Applications list of Applications hosted in India would issue orders to block them in India.

c) Regulatory body would collaborate with App markets and ensure that such malicious Apps are taken down and action taken against such developers. It would also ensure that Apps developed by people whose provenance is mysterious are not allowed to be downloaded in India.

d) As we have discussed in the foregoing social media platforms are the most favourite terrain for deploying and distributing malicious applications. A Crime can always take place irrespective of whether the social media platform is secure or not, but what is more appalling is the lackadaisical attitude of the social media platform administrators in not co-operating with Law Enforcement Agencies, investigating the crime to bring the culprits to book. Most of these social media platforms like Facebook, Twitter, WhatsApp, Telegram etc are owned by companies who are incorporated in United States of America and claim to be governed by Section 230 of the Communications Decency Act (CDA) of 1996 (a common name for Title V of the Telecommunications Act of 1996), a piece of Internet legislation in the United States, codified at 47 U.S.C. § 230, consequently they have an arrogant attitude toward the requests made by the citizens and Law Enforcement Agencies and try to obstruct administration of justice and investigation by not providing critical information in time. As social media platforms can be accessed only through search engines on internet, the role of TSPs and ISPs cannot be understated in minimising the exploitation of App Ecosystem for cybercrimes. The following are suggested in this regard:

i) As cyberspace has been acknowledged as the fourth domain of Warfare after Land, Sea and Air, the foremost requirement for operations of these social media platforms should be to run their Indian operations by incorporating a Company in India over which the jurisdiction and laws of India apply. The Chief Executive Officer of the Indian Company should be an Indian passport holder and ordinarily be a resident in India. By implementing this provision social media platforms would be under jurisdiction of Indian criminal and civil law. This would strategically give India some perceived control over the Cyberspace.

ii) All the servers related to the Indian user's data or at least their mirrors must be kept and installed in India only. The passwords of these clouds spread over several international jurisdictions may be kept in an escrow account.

iii) License from MeitY must be made compulsory for their operations in India. They should be treated as service providers, under the licensing conditions, who should be bound by the directions of MEITY for regulating their operations in India. The violations of the instructions issued by MEITY in accordance with the terms and conditions of the licence would result in cancellation of the licence to operate as also make them liable for criminal and civil suit.

iv) Automated repository of the mobile numbers to which the account was linked must be shared with and maintained by an Agency of Ministry of Home Affairs so that it can be verified with the service provider to help trace the misuse of social media accounts and also find a fake one.

v) While creating an account on any of these social media platforms it should be mandatory for the user to verify his or her credentials including mobile number through net banking or a credit card to establish his rightful coordinates, in case of any investigation. Minimum amount of ₹1 or ₹10 may be deducted for a confirmed transaction for establishing the credentials of the user by the Bank. If the bank account is inactive for more than 3 months, the Bank should not process this confirmation request. This suggestion is important because it would take care of several fake handles run by Criminals, Naxals and Anti-National elements thus also preventing the spread of fake news by these suspect handles.

vi) Provision for heavy financial penalties including cancellation of operations and imprisonment of the officials of the social media platforms should be made, if they don't comply with the requests of Law Enforcement Agencies for investigation and data requests or request for removal of data by the LEA.

BIBLIOGRAPHY

[1] Arjun Chetry, & Uzzal Sharma. (2023). *Anonymity in decentralized apps: Study of implications for cybercrime investigations.* Guwahati: International Academic Publishinh House. Retrieved from https://pdfs.semanticscholar.org/0a7d/1348bd539be4e9d48542f7509c76d439fac7.pdf?_gl=1*19bgt9v*_gcl_au*MTY5Nzg1NjI1Mi4xNzMxNDAyMzM1*_ga*MTk0Njc0NjYyNS4xNzMxNDAyMzM3*_ga_H7P4ZT52H5*MTczMTQwMjMzNi4xLjEuMTczMTQwMzE5MC42MC4wLjA.

[2] Chang Yue, Chen Zhong, Kai Chen, Zhiyu Zhang, & Yeonjoon Lee. (1999). *DARKFLEECE: Probing the Dark Side of Android Subscription Apps.* Retrieved from https://www.usenix.org/system/files/sec24fall-prepub-2543-yue.pdf

[3] Chen, Z. a. (2021). *Lifting The Grey Curtain: A First Look at the Ecosystem of CULPRITWARE.*

[4] Haoyu Wang, Zhe Liu, Jingyue Liang, Narseo Vallina-Rodriguez, Yao Guo, Li Li, . . . Guoai Xu. (2018). Beyond Google Play: A Large-Scale Comparative Study of Chinese Android App Markets. Association for Computing Machinery. Retrieved from https://dl.acm.org/doi/10.1145/3278532.3278558

[5] Liu Wang, Haoyu Wang, Ren He, Ran Tao, Guozhu Meng, Xiapu Luo, & Xuanzhe Liu. (2022). MalRadar: Demystifying Android Malware in the New Era. *ACM SIGMETRICS Performance Evaluation Review.* Retrieved from https://www.researchgate.net/publication/361849753_MalRadar_Demystifying_Android_Malware_in_the_New_Era

[6] Luman Shi, Jiang Ming, Jianming Fu, Guojun Peng, Dongpeng Xu, Kun Gao, & Xuanchen Pan. (2020). VAHunt: Warding Off New Repackaged Android Malware in App-Virtualization's Clothing. New York: Association for Computing Machinery. Retrieved from https://dl.acm.org/doi/10.1145/3372297.3423341

[7] Shuichi Ichioka, Estelle Pouget, Takao Mimura, Jun Nakajima, & Toshihiro Yamauchi. (2020). Accessibility Service Utilization Rates in Android Applications Shared on Twitter. Japan. Retrieved from https://www.researchgate.net/publication/347456757_Accessibility_Service_Utilization_Rates_in_Android_Applications_Shared_on_Twitter

[8] Surisetti, P. (2017). *Code 2.0 Chapter Review. #Technology, IP and Regulation.* Retrieved from SpicyIP: https://spicyip.com/2017/07/code-2-0-chapter-review-technology-ip-and-regulation.html

[9] theuncertaintyproject. (2002). *rumsfeld-matrix.* Retrieved from theuncertaintyproject: https://www.theuncertaintyproject.org/tools/rumsfeld-matrix

[10] Zhuo Chen, Lei Wu, Jing Cheng, Yubo Hu, Yajin Zhou, Zhushou Tang, . . . Kui Ren. (2021). *Lifting The Grey Curtain: A First Look at the Ecosystem of CULPRITWARE.* Retrieved from https://arxiv.org/abs/2106.05756