Arraid Journal of Science and Technology (AJST)
Higher Institute of Science and Technology-Al Shmokh

مجلة الرائد للعلوم والتقنية
المعهد العالي للعلوم والتقنية ـ الشموخ

Received: 20 Sep 2025 | Accepted: 10 Nov 2025 | Published Online: 31 Dec 2025

Detecting Profile Cloning Attack in Social Networks

Ismail Mohamed Aburagaga and Mohamed Muftah Abubaera *
Data Analytics Department, Elmergib University
* Computer Department, Elmergib University
Contact Information: E-mail: imaburagaga@elmergib.edu.ly

ABSTRACT
Profile cloning, one of the most common forms of digital identity fraud, refers to the intentional imitation of a user's personal social network accounts by creating a false one in order to make a fake account. This manipulative approach takes advantage of the trust and interrelation properties of SNS architecture to facilitate various cyber-attacks, such as impersonation, social engineering, phishing, and false information campaigns and fake news. Herein, we present an extensive discussion on the phenomenon of profile cloning. It starts with an introduction explaining profile cloning and differentiating it from related attacks such as identity theft or catfishing. The paper goes on by outlining the primary cloning methods, Friend-List-based Cloning and Full-Profile Cloning. It examines both the primary motives that drive the perpetrators with anything from financial fraud and societal sabotage, all the way to espionage and vendettas. Key to this analysis is its focus on the multi-faceted effects upon victims, organizations, and social media in general, as well as on the psychological, financial, and reputational impacts. The paper then provides an overview of detection methods and how various approaches cover user-centric methods, feature-based machine learning methods, and graph-based analytical methods. It also analyses the legal and ethical systems today and describes problems with jurisdictional enforcement and platform accountability. In conclusion, the paper synthesizes proactive and strategic mitigating approaches by users, SNS providers, and the policy community in order to find that a multi-stakeholder response by means of high-tech detection, robust legal representation, and ongoing teaching and promoting digital literacy is critical to the efforts of responding to the growing threat posed to online identity and trust.

KEYWORDS: Profile cloning, social network security, identity theft, cybersecurity, trust, online fraud, detection algorithms.

1. INTRODUCTION

The advent of social networking sites (SNSs) has fundamentally reshaped human interaction, creating a globally interconnected digital society. Platforms like Facebook, X (formerly Twitter), LinkedIn, and Instagram have become central to how individuals construct identity, maintain relationships, access information, and conduct business [1]. This digital socialization, however, occurs within an architecture built on a currency of trust. Users inherently trust that the profiles with which they interact are authentic

representations of real individuals or entities. It is this very trust that malicious actors seek to exploit through a deceptive practice known as profile cloning. In the last few years, billions of users actively engage on these platforms to share life events, opinions, and professional achievements, and to maintain social ties [2]. This unprecedented volume of personal data, however, has turned SNSs into lucrative targets for malicious actors. Among the various forms of online deception, profile cloning has emerged as a significant and growing threat to user trust and safety.

Profile cloning, also referred to as identity cloning or social cloning, is the process of creating a fake profile on a social network by copying the public-facing identity elements of a legitimate user [3]. The cloner harvests publicly available information such as profile pictures, display names, biographical data, and even entire photo albums to construct a convincing digital doppelganger of the victim. This clone profile is then used to send friend requests to the victim's actual contacts, leveraging the pre-existing trust relationships to gain acceptance into their social circle [4]. Once integrated, the cloner can engage in various malicious activities.

The fundamental difficulty in managing the challenge of profile cloning lies in its deceptive simplicity. For the victim’s circle of friends, a cloned profile appears authentic, making it difficult to distinguish from the genuine account without close inspection. This is compounded by the immense magnitude of social networks, which makes manual monitoring by platform providers impractical. Thus, there is the need for automated, rapid, and precise detection systems [5].

The prevalence of this issue is staggering. While precise global figures are elusive due to underreporting, data from platform transparency reports indicate that Facebook actioned billions of fake accounts in a single year, a category that includes cloned profiles [6]. The motivation behind this deceptive practice is not monolithic; it ranges from financial scams and corporate espionage to personal harassment and large-scale influence operations [7]. The consequences for victims are severe, encompassing emotional distress, financial loss, reputational damage, and a lasting erosion of trust in online communities [8].

This paper aims to provide a holistic and in-depth examination of profile cloning in social networks. It will dissect the attack vector by first clarifying its definition and distinguishing it from related concepts. The methodologies employed by cloners will be detailed, followed by an exploration of their diverse motivations. The profound impacts on various stakeholders will be analyzed to underscore the seriousness of the threat. The paper will then transition to the defensive front, reviewing the current state of detection technologies, from user-reported flags to sophisticated machine learning algorithms. The legal and ethical landscape surrounding this issue will be scrutinized, highlighting the gaps between technological malfeasance and legal recourse. Finally, the paper will propose a consolidated framework of mitigation and prevention strategies, arguing that effectively combating profile cloning requires a synergistic effort from individual users, SNS platforms, and regulatory bodies.

2. DEFINING PROFILE CLONING

Profile cloning: a digital form of impersonation. To comprehend these mechanisms and threat factors more intricately, it is important to isolate it from other, similarly connected forms of online deception.

2.1. Core Definition

Profile cloning involves the unauthorized reproduction of an identity of someone or an organization on the popular social network to create a phony account. The clone profile is not originally generated but a reflection, meant to be indistinguishable from the real profile to the victim's social contacts [3]. The key differentiator is the targeted nature of the attack; the cloner selects a specific victim whose social graph they wish to infiltrate.

2.2. Distinction From Related Attacks

Identity Theft: While profile cloning is a form of identity theft, the term identity theft in a broader context often refers to the theft of personally identifiable information (PII) like Social Security numbers, credit card details, or medical records for primarily financial gain [9]. Profile cloning, in contrast, primarily steals the victim's social identity and their network of trust to enable other crimes.

Catfishing: Catfishing involves creating an entirely fictional online persona, often using a composite of stock photos or stolen images from a non-consenting individual who is not the attacker's target. The goal is typically to initiate a deceptive romantic relationship [10]. In profile cloning, the persona is not fictional; it is a direct copy of a real person, and the target is not the victim themselves, but their friends.

Botnets and Sybil Attacks: Botnets consist of armies of automated accounts controlled by a single entity, often used for spam distribution or amplifying disinformation [11]. A Sybil attack involves one entity creating multiple fake identities to undermine a peer-to-peer system's reputation structure [12]. While a cloner may use automated tools, the cloned profile itself is often operated manually or semi-manually to maintain the illusion of authenticity, and its power derives from mimicking a single, specific real user.

2.3. Primary Cloning Methodologies

Researchers have discovered two main technical techniques for implementing a profile cloning attack:

Friend-List-based Cloning (Cross-site Cloning): This is one of the most common forms. In this type of tactic, the attacker finds a victim on one social network (e.g., Facebook, where privacy settings are strict) and uses their publicly available information (name, profile picture) to set up a clone profile on a different social network (e.g., Instagram or Twitter, where the victim may not be present or has a less-secured profile) [4].The cloner then imports the victim's public friend list from the original platform and sends connection requests, often with a message like "I'm new here, add me!" This exploits the fact that friends assume the victim has genuinely joined a new platform.

Full-Profile Cloning (or Intra-site Cloning): This more brazen attack occurs on the same social network. The attacker creates a new profile on the same platform as the victim, replicating all publicly accessible content. This is often successful when the

victim's privacy settings are lax, allowing the cloner to copy photos, posts, and biographical information. As platform algorithms are often used for duplicate account detection purposes, cloners may make changes to a person's profile such as the display name, such as using a middle initial, or image-editing to change the profile picture subtly to evade initial detection [13].

3. MOTIVATIONS BEHIND PROFILE CLONING

Understanding the "why" behind profile cloning is essential for developing effective countermeasures. The motivations are as diverse as the perpetrators themselves.

3.1. Financial Fraud and Scams

This is arguably the most common motivation. Once the clone profile is accepted by the victim's friends, the cloner can initiate various scams:

The Emergency Scam (or "Grandparent Scam"): The cloner sends messages to the victim's friends or relatives, claiming to be in a sudden crisis (e.g., stranded in a foreign country, arrested, or in a medical emergency) and urgently needing money to be wired [14].

Phishing and Credential Harvesting: The clone account can send links to fake login pages for popular services, tricking friends into entering their usernames and passwords under the guise of "checking out this video" or "verifying your account" [7].

Promotion of Fake Goods and Services: The trusted identity is used to endorse or sell counterfeit products, fake event tickets, or fraudulent investment schemes.

3.2. Social Engineering and Espionage

In a corporate or political context, profile cloning is a powerful tool for social engineering.

Corporate Espionage: A cloner can target employees of a competitor company, clone their LinkedIn profile, and use it to connect with other employees to extract sensitive information about projects, strategies, or internal vulnerabilities [15].

Spear Phishing for Network Access: By cloning the profile of an IT administrator or a high-level executive, attackers can send targeted emails or messages to other employees, tricking them into installing malware or divulging network credentials, which can serve as an entry point for a larger cyber-attack [16].

3.3. 2.3 Social Sabotage and Harassment

Profile cloning is frequently weaponized for personal vendettas, bullying, and reputation damage.

Defamation: A malicious actor can clone a victim's profile and use it to post offensive, controversial, or illegal content. This can damage the victim's personal relationships, professional reputation, and even lead to real-world consequences like job loss or legal trouble [17].

Harassment and Cyberbullying: The clone can be used to send abusive messages to the victim's friends or to engage in trolling behavior, with the blame falling on the innocent victim. This can cause significant psychological distress [8].

3.4. Information Warfare and Influence Operations

State-sponsored actors or political groups use profile cloning as part of larger disinformation campaigns.

Astroturfing: Cloned profiles, often managed in concert with bots, are used to create a false impression of widespread public support or opposition for a political candidate, policy, or idea. These accounts amplify specific narratives and attack opponents, polluting the digital public square [18].

Sowing Discord: By cloning profiles of individuals from different ideological groups, actors can infiltrate communities and post inflammatory content designed to exacerbate social and political divisions.

4. THE MULTI-FACETED IMPACTS OF PROFILE CLONING

Profile cloning inflicts considerable harm beyond a mere nuisance; the harm in practice is real and often catastrophic for people, companies, and society as a whole.

4.1. Impacts on Individual Victims

Psychological and Emotional Distress: Finding out that your identity has been stolen and co-opted against friends and family members can be an incredibly violating experience. Victims say they feel anger, anxiety, helplessness, and a lack of personal security. Reclaiming one’s digital identity can be frustrating and re-traumatizing [8]. The social fallout from any malicious posts made by the clone can also lead to social isolation and depression.

Financial Loss: As outlined in the motivation section, cloning victims can personally be financially disadvantaged if their contacts fall for emergency scams. In addition, they could pay the cost of legal advice, credit monitoring services, and the extensive time that it would take to reach a resolution [14]**.**

Reputational Damage: The most pernicious impact can be the erosion of a victim’s reputation. Malicious posts, scams, or simply the confusion sown by the existence of a duplicate profile can lead to a loss of trust among friends, colleagues, and professional contacts. Repairing a damaged reputation can be a long and difficult process [19].

4.2. Impacts on Organizations

Reputational and Brand Damage: If a high-profile executive or the official corporate account is cloned and used for malicious purposes, it can severely damage the organization's public image and shareholder confidence.

Financial and Intellectual Property Loss: Successful social engineering attacks via cloned profiles can lead to direct financial theft (e.g., manipulated wire transfers) or the loss of valuable intellectual property, giving competitors an unfair advantage [15].

Compromised IT Security: A single successful spear-phishing attack initiated from a cloned profile can serve as the initial breach that leads to a full-scale network compromise, including ransomware attacks or data breaches.

4.3. Impacts on the Social Media Ecosystem

Erosion of Trust: This is the most significant systemic impact. The pervasive use of cloned profiles and other fake accounts fundamentally erodes the trust that is at the root of social networking. Without any level of assurance to the user that the person they are interfacing with is genuine, it degrades the quality of discourse, discourages authentic engagement, and may ultimately drive users away from the platform [20].

Pollution of the Information Environment: Cloned profiles used in disinformation campaigns contribute to the spread of falsehoods and make it increasingly difficult for citizens to access reliable information, with dire consequences for democratic processes [18].

5. DETECTION OF CLONED PROFILES

To confront profile cloning, people need multi-faceted measures of detection that leverage both human vigilance and the automation of the system.

5.1. User-Centric Detection

The first line of defence is often the users themselves.

Friend Vigilance: Victims' friends may detect a clone by receiving a duplicate friend request from someone they are already connected to, or by noticing subtle discrepancies in the new profile, such as a lack of historical posts, a small number of friends, or anomalous communication style [21].

Victim Discovery: Victims may discover they have been cloned through reports from friends, by conducting periodic self-searches on different platforms, or by using third-party services that monitor for impersonation.

5.2. Feature-Based Machine Learning Detection

SNS platforms deploy sophisticated machine learning (ML) models to identify fake and cloned accounts proactively. These models typically analyze a wide array of profile features:

Profile Features: The completeness of the profile, the age of the account, the use of default images, and the ratio of followers to follow [22].

Content-Based Features: The linguistic patterns of posts and messages, the rate of posting, and the similarity of posted content to other known sources [23].

Network Features: The structure of the user's social graph. Clone accounts often exhibit anomalous growth patterns, rapidly sending out a large number of friend

requests with a low acceptance rate. They may also be disconnected from expected community structures [24].

A typical ML pipeline involves feature extraction, training a classifier (e.g., Random Forest, Support Vector Machines) on a dataset of known legitimate and fake accounts, and then using the model to score new accounts for their likelihood of being fraudulent [25].

5.3. Graph-Based and Behavioral Analysis

More advanced detection systems move beyond individual profile features to analyze relational and behavioral patterns.

Graph Similarity Analysis: This technique directly addresses profile cloning by comparing the social graph and profile attributes of a new account against all existing accounts. If a high degree of similarity is found (e.g., matching profile pictures and a significant overlap in friend lists), the new account is flagged as a potential clone [3].

Behavioral Biometrics: Studying micro-patterns of user behavior, including mouse movements, typing rhythm, and typical login times, can help differentiate a human-driven legitimate account from a potentially malicious one, even if the profile content is identical [26].

However, even with these sophisticated methods, detection remains a challenging arms race. That is, clone accounts continuously adapt their methods to evade detection allowing new clone accounts to "age," for example, or operating them manually to mimic human behavior more closely.

6. LEGAL AND ETHICAL CONSIDERATIONS

The legal landscape for addressing profile cloning is complex and often lags behind the pace of technological change.

6.1. Legal Frameworks and Jurisdictional Challenges

Computer Misuse and Identity Theft Laws: Many countries have laws that prohibit unauthorized computer access and identity theft. Similarly, in the United States, the Computer Fraud and Abuse Act (CFAA) and individual state-level identity theft statutes may be applied to profile cloning [27]. But prosecuting a case goes beyond catching the person responsible — which is often difficult — to proving that the defendant caused sufficient harm to sustain prosecution; such a threshold can be high.

Defamation and Harassment Laws: If the clone is used for defamatory or harassing purposes, victims can pursue civil actions. But again, the anonymity of the cloner is a major obstacle, and the global nature of the internet creates jurisdictional nightmares [17]. A cloner operating from one country can target a victim in another, using a platform headquartered in a third, making legal recourse incredibly complex.

Platform Terms of Service: The primary and most immediate form of "law" on SNSs is the platform's Terms of Service (ToS), which universally prohibit impersonation. Victims can report cloned profiles, and platforms will typically remove them for

violating ToS. However, this is a reactive, after-the-fact measure and does not deter or punish the cloner.

6.2. Ethical Responsibilities of SNS Platforms

Ongoing debate over social media companies' ethical obligations to prevent harm on their platforms.

Duty of Care: Criticism is that platforms have an ethical (if not yet fully legal) "duty of care" to design their systems to reduce the potential of harms, which can include profile cloning. This can include implementing more rigorous identity verification (without compromising user privacy) and investing in more preemptive detection solutions [28].

Transparency and Redress: Ethically, platforms owe their users transparency about the policies they adopt and clear, accessible channels for redress when problems occur. The often-opaque and automated process of reporting and account suspension can itself be a source of user frustration and perceived injustice [29].

7. MITIGATION AND PREVENTION STRATEGIES

A comprehensive solution to profile cloning requires a tripartite approach involving users, platforms, and policymakers.

7.1. User-Centric Mitigation

Empowering users is the first and most accessible layer of defence.

Privacy Hygiene: Users should regularly audit and tighten their privacy settings. The principle of least privilege should apply: information should only be visible to friends or custom lists, not to the public. This drastically reduces the amount of data a cloner can harvest [9].

Digital Literacy and Awareness: Public education campaigns are crucial. Users need to be taught to be skeptical of duplicate friend requests, to verify identities through secondary channels (e.g., a phone call or a separate messaging app), and to recognize the hallmarks of common scams.

Proactive Monitoring: Users should periodically search for their own name on major social platforms to check for impersonation accounts. Google Alerts for one's own name can also provide an early warning.

7.2. Platform-Centric Solutions

SNS providers bear the primary responsibility for deploying technical countermeasures.

Advanced Proactive Detection: As discussed, continued investment in and refinement of ML and graph-based detection algorithms is non-negotiable. This includes developing models that are more resilient to adversarial evasion techniques.

Robust Identity Verification (with Caveats): On one hand, there are controversial, mandatory real-name policies which could damage marginalized users; on the other, it might also be helpful to have optional, privacy-preserving forms of verification. For example: the possibility to cryptographically verify the ownership of a profile across multiple platforms is an action to be taken as a counter to cross-site cloning [30].

Streamlined Reporting and Victim Support: Platforms must create more user-friendly, transparent, and responsive reporting systems. Dedicated support channels for victims of serious impersonation can significantly reduce the time and stress involved in resolving these incidents.

7.3. Policy and Legal Interventions

Governments and international entities must play an important role in promoting a safer online environment.

Harmonization of Cybercrime Laws: International cooperation to harmonize laws against online impersonation and identity theft would help overcome jurisdictional hurdles and facilitate cross-border investigation and prosecution.

Platform Accountability Regulations: Legislatures are increasingly considering regulations, such as the EU's Digital Services Act (DSA), that would mandate platforms to conduct risk assessments and take measures to mitigate systemic risks, which could include the risk posed by impersonation and fake accounts [31]**.**

Support for Digital Literacy Initiatives: Governments could fund and champion national digital literacy curricula that include instruction about cybersecurity threats such as profile cloning.

8. CONCLUSION AND RECOMMENDATIONS

Profile cloning is a high-tech, destructive cyberattack to the trust which lies behind modern social networks. While it is not one type of crime, it has become an adaptable attack vector with diverse adverse uses including petty fraud, sabotage, and geopolitical influence operations. It seriously affects victims of these online predators, with psychological, financial, and/or reputation consequences, the effects reaching the public sphere and undermining trust in digital public spaces and information ecosystems. The war against this digital doppelgänger is a continuous arms race. While users can and certainly should exercise improved privacy protocols, it ultimately falls to social networking platforms to take advantage of sophisticated and advanced tech—such as feature-based machine learning and graph similarity analytics to be able to pre-emptively flag and dismantle cloned profiles. And the current legal frameworks are often insufficient to tackle the transnational, anonymous nature of these crimes, demanding broadened international engagement and possibly new regulatory strategies, which compel platforms to adopt safer systems. It has to end with the goal of decreasing the potential threat of profile cloning, it is crucial that a concerted effort by anyone working in all quarters. Individuals need to be digital vigilant, technology companies need to invest in ethical and effective security engineering and legislators and technocracies need to make sophisticated laws to protect citizens without quelling innovation or free speech. Only if we approach this complexity with a multi-pronged approach can we maintain the integrity of online identity and create social media spaces in which trust works.

REFERENCES

[1] N. B. Ellison and D. M. Boyd, "Sociality through social network sites," in *The Oxford Handbook of Internet studies*, W. H. Dutton, Ed. Oxford University Press, 2013, pp. 151-172.
[2] A. Smith and M. Anderson, "Social Media Use in 2023," Pew Research Centre, 2023.
[3] M. Conti, R. Poovendran, and M. Secchiero, "Facebook: Detecting fake profiles in on-line social networks." *in Proceeding 2012 IEEE/ACM Int. Conf. Adva.in Social Netw. Anal. & Min.,* 2012, pp. 1071-1078.
[4] L. Bilge, T. Stufe, D. Balzarotti and E. Kirda, "All your contacts are belong to us: Automated identity theft attacks on Social Networks," *in Proceeding 18th Int. Conf. World Wide Web,* 2009, pp. 551-560.
[5] M. Fire. R. Goldschmidt, and Y. Elovici, "Online Social Networks: Threats and Solutions," *IEEE Commun. Surveys Tuts.,* vol. 16, no. 4, pp. 2019-2036, 2014.
[6] Facebook, "Community Standards Enforcement Report," 2022. [Online]. Available on https://transparency.fb.com/data/community-standards-enforcement/
[7] T. N.Jagatic, N. A. Johnson, M. Jakobsson, and F. Menczer, "Social Phishing, "*Commun. ACM,"* vol. 50, no. 10, pp. 94-100, Oct. 2007.
[8] J. T. Hancock, K. Birch, and E. Cage, "The consequences of online deception for victims and perpetrators," *Curr. Opin. Psychol*. Vol. 36, pp. 106-111, 2020.
[9] R. Gross and A. Acquisti, "Information revelation and privacy in online social networks," in *Proc. 2005 ACM Workshop Privacy Electron. Soc.,* 2005, pp. 71-80.
[10] V. Lukacs, *The Catfish Effect: A Study of Deception in online Dating.*London, UK: Palgrave Macmillan, 2019.
[11] C. Freitas, F. Benevenuto, S. Ghosh, and Veloso, "Reverse engineering socialbot infiltration strategies in Twitter," in *Proc. 2015 IEEE/ACM Int. Conf. Adv. Soc. Netw. Anal. Min. (ASONAM),* 2015, pp. 25-32.
[12] J. R. Douceur, "The Sybil attack," in *Int. Workshop Peer-to-Peer Syst.,* 2002, pp. 251-260.
[13] A. K. Jain, Social Network Forensics: Emerging Research and Opportunities. Hershey, PA: IGI Global, 2017.
[14] M. Button, C. Lewis, and J. Tapley, "A Better Deal for Fraud Victims: Research into Victims" Needs and Experiences. Portsmouth. UK: University of Portsmouth, Centre for Counter Fraud Studies, 2014.
[15] F. L. Greitzer, D. A. Frincke, and M. Zabicki, "Using social network analysis for counter-terrorism." in *Proc. 2008 IEEE Conf. Technol. Homeland Secur.,* 2008, pp. 41-46.
[16] S. Gupta, Social Engineering: The Science of Human Hacking, 2nd ed. Hoboken, NJ: John Wiley & Sons, 2019.
[17] D. K. Citron, *Hate Crimes in Cyberspace*. Cambridge, MA: Harvard University Press, 2014.
[18] S. C. Woolley and P. N. Howard, *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media.* Oxford, UK: Oxford University Press, 2019.
[19] D. J. Solove, "*The Digital Person: Technology and Privacy in the Information Age.* New York, NY: NYU Press, 2004.
[20] C. Dwyer, S. R. Hiltz, and K. Passerini, "Trust and Privacy concern within social networking sites: A comparison of Facebook and MySpace." in *Proc. AMCIS 2007,* 2007, p. 339.
[21] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in *Proc. 26th Annu. Comput. Secur. Appl. Conf.,* 2010, pp. 1-9.
[22] S. Guarajala, J. S. White, B. Hudson, and J. B. Voter, "Profile characteristics of fake Twitter accounts, "*Big Data Soc*., vol. 3, no. 2, pp. 1-13, 2016.

[23] K. Lee, B. D. Eoff, and J. Caverlee, "Seven months with the devils: A long-term study of content polluters on Twitter," in *Proc, Int AAAI Conf, Web Soc. Media,* vol. 5, no. 1, 2011, pp. 185-192.
[24] Y. Boshmaf, I> Muslukhov, K. Beznosov, and M. Ripeanu, "The Socialbot network: When bots socialize for fame and money," in *Proc. 27th Annu. Commput. Secur. Appl. Conf.,* 2011, pp. 93-102.
[25] E. Van der Walt and J. H. Eloff, "Using machine learning to detect fake identities: Bots vs humans." *IEEE Access,* vol. 6, pp. 6540-6549, 2018.
[26] C. Shen, L. Xu, X. Cheng, Q. Cao, and S. Wen, "A behavioral biometrics-based user verification for social networks," *IEEE Trans. Comput. Soc. Syst.,* vol. 6, no. 3, pp. 516-525, Jun 2019.
[27] O. S. Kerr, "Norms of computer trespass," *Columbia Law Rev.,* vol. 116, no. 4, pp. 1143-1185, 2016.
[28] T. Gillespie, *Custodians of the Internet: Platforms, Content Moderation, and the Hidden Decisions that Shape Social Media.* New Haven, CT: Yale University Press, 2018.
[29] S. Myers West, "Censored, Suspended, Shadow banned: User Interpretations of content moderation on social media platforms," New Media Soc., vol. 20, no. 11, pp. 4366-4383, 2018.
[30] Y. Zhang, "A decentralized identity-based social network, "in Proc. 2020 IEEE 6th Int. Conf. Comput. Commun. (ICCC). 2020, pp. 2234-2238.
[31] European Commission, "The Digital Services Act: Ensuring a safe and accountable online environment," 2022. [Online]. Available on: http://ec.europe .eu/commission/presscorner/detail/en/qanda_22_2543.