MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 2309-2315

ANONYMITY TO EXPOSURE: THE PITFALLS OF DOXING IN MODERN ERA

Itisha Bhoi [1] and **Dr. Madhubrata Mohanty** [2]
[1,2]*Faculty of Legal Studies, SOA National Institute of Law,*
Siksha O' Anusandhan (Deemed to be) University, Bhubaneswar, Odisha, India.
[1]Email: itisha2211@gmail.com ORCID ID: 0009-0007-9579-4147
[2]Email: madhubratamohanty@soa.ac.in ORCID ID: 0000-0001-6482-4824

ABSTRACT
Doxing, the malevolent method of revealing someone's personal information in public without their consent, is an alarming threat to privacy and safety in the digital as well as analogue world. The advancement of social media has resulted in easy accessibility and availability of information, thereby increasing the risks associated with Doxing. Doxing has been one of the overlooked offences committed under the radar which infringes the right to free speech, causes psychological turmoil among people and undermines their confidence in engaging on online public platforms or voicing opinions. This paper offers an expanded account of doxing as a multifaceted social and legal phenomenon. It outlines the common tactics like widespread data exposures, coordinated campaigns, targeted leaks adopted by the perpetrators and the motivation behind such acts. It maps the harm experienced by the victims, such as financial loss, emotional distress, loss of reputation, defamation and also discusses the ramifications of Doxing on the family members of the victims. Some countries have enacted specific laws against this transgression, while others, including India, still rely on broader laws related to privacy and cyber crimes. The study highlights the need for a clear and precise definition of doxing to enhance the effectiveness of justice delivery system. Furthermore, the study emphasizes the diverse strategies adopted by various nations, explores the global legal landscape of legislation in addressing doxing and measures the effectiveness of the existing legislation. Additionally, certain suggestive measures like need for awareness programme, collaboration of IT and law departments, need for stringent regulation have been highlighted to curb the problem. In the end, it reinforces the necessity of thorough legislation that not only safeguards individuals but also conforms to the fast-evolving nature of online threats.
Keywords: Data, Doxing, Legislation, Personal information, Privacy

1. Introduction

It would be truly horrendous to imagine an individual waking up to a mob in front of their house waiting to hurl abuses, cause physical harm and stalk them or their family members. This is the outcome of mishandling digital platforms. The ability to control one's information is a key aspect of an individual's identity. Individuals are willing to go to extremes to protect their data and taking advantage of this, the perpetrators illegally try to access data to manipulate and use it against the victims to achieve their motives. It concerns that individuals' personal data is circulated worldwide and thereafter used to locate them in real-time and in person. This act, which we are ignorant about, eventually leads to an offense termed as Doxing. Doxing is a neologism that has gained attention in the current scenario and is being gradually accepted into the mainstream language. This term had its origins two decades ago when the term 'dropping dox' or 'docs' emerged. Thereafter, documents that were dropped by internet users on online platforms to reveal the identity of individuals resulted in the term 'Doxing'. This offence was amplified during the COVID-19 era. In those days, online platforms posed an important medium for exchanging ideas and views by connecting people around the world. Subsequently, there was a proliferation of users on online platforms like Twitter, Facebook, Instagram, LinkedIn, etc. Although such platforms facilitated the free flow of information but resulted to be an easier medium for exchanging hateful comments, dis-likeness, and instant retaliation amongst individuals who had diverse opinions. People would sit behind computers, laptops and mobiles in their homes and use technology in a hassle-free manner. Thus, when there was a difference in opinion about the preconceived notion of a certain topic, or if it involved racist or rude behaviour, then the internet users admonished, criticized and resorted to bullying which, also included public disclosure of personal information about the victim. Such disclosure which, was detrimental to the safety and security of the individual, resulted in an offence known as Doxing.

2. Review of Literature

It is pertinent to note that, regardless of direct data breaches, perpetrators take advantage of publicly available information and weak digital footprints to attack the victims, leading to consequences such as psychological harm, identity theft and threats to the personal safety of individuals. Similarly, the "Purpose limitation principle" states that when information is collected for some purpose, it should be used for that particular purpose only and not for any unrelated purpose. Kukul (2023) suggests that doxing violates the purpose limitation principle which, prohibits the dissemination of public or private information for malicious purpose and goes beyond the invasion of privacy while posing a risk to one's confidentiality, dignity and other fundamental rights, advocating for a comprehensive legal framework. Furthermore, the authors highlight the creation of a "legal vacuum" due to the absence of anti-doxing legislation. This vacuum interferes with victim restitution and overlooks the malicious accumulation of data (Pratama & Sari, 2024). In addition to this, several studies indicate that perpetrators collect various fragmented pieces of information and use such information to create a detailed profile of an individual which, is often called as "data aggregation"(Meyer, 2024). A report by PEN America emphasizes the magnitude of online harassment and the ineffectiveness of reporting systems on digital platforms. Users often consider the system as worthless and term it as "shouting into the void" due to a lack of transparency, accountability and prompt response (PEN America, 2023). The study also highlights how inadequate reporting systems fail to protect victims as well as dissuade them from seeking justice, which contributes to further harm and undermines security on the internet. According to Amnesty International, a considerable number of activists who are young experience harassment on online platforms, followed by offline or physical violence. Three out of five child and young activist face harassment online, based on the analysis (Amnesty International, 2024). Additionally, this kind of harassment creates an environment of fear, undermines the freedom of expression of the individuals and simultaneously discourages from voicing out opinions. As indicated in another study, doxing was prevalent among adolescents and victims experience constant stress, exhibit symptoms of depression and anxiety. The study also emphasizes that disclosure of personal information online intensifies mental anguish and raises the vulnerability of victims (Chen et al., 2018).

3. Research Problem

This study addresses the problem of regulatory inadequacy and enforcement gaps in recognizing doxing as a separate offence. Due to the growth of digital platforms and online anonymity, the issue of doxing has been common yet insufficiently addressed by current legal frameworks despite its grave consequences. Hence, the study takes a look at these discrepancies and determines the importance of adequate legal oversight.

4. Objectives of Research

- To examine the concept of anonymity and forms of doxing and how it undermines the foundations of privacy and individual autonomy.
- To study the impact and consequences of doxing on individuals.
- To evaluate existing legal frameworks governing doxing in various nations and identify the shortcomings in regulating this problem.

5. Research Methodology

The study adopts a doctrinal research methodology and analyses various legal provisions, legal principles, judicial decisions and existing statutes related to doxing and data protection laws. The research relies on secondary sources for collection of data. It refers various journal articles, reports, case laws and legislations. The study also incorporates comparative approach by examining legal frameworks of different countries and their regulatory practices.

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 2309-2315

6. Concept of Doxing

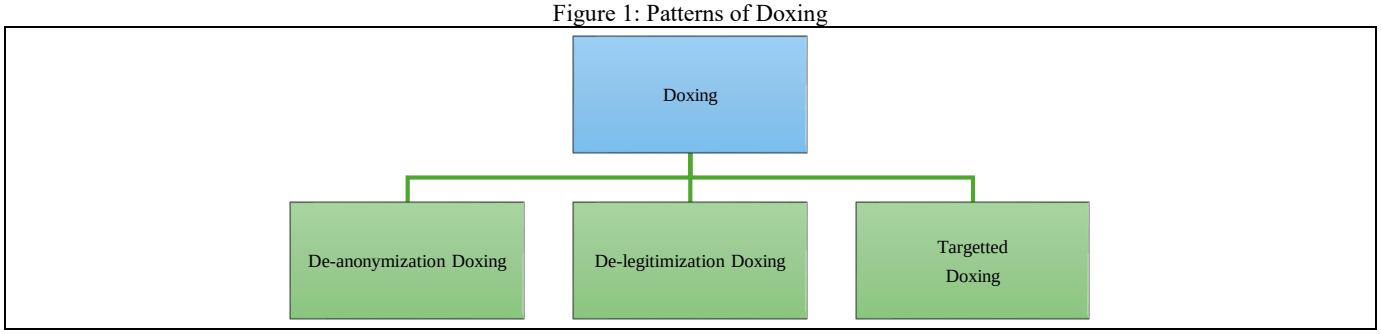
In common parlance, Doxing is a form of revealing information relating to the personal identification of an individual without his/her consent, which is sufficient in the ordinary course to locate such an individual. This act is done by using the Internet and other online platforms. Personal information may include phone numbers, social security numbers, medical records, email addresses, residence addresses, workplace addresses, financial details, employment information etc. "When various identifiable information is gathered about a person, creating a dossier about that individual may be said to be the outcome. This entails gathering, preserving, using, and sharing the personal information of individuals."[1]

The Value of Anonymity:

One important asset of an individual in the current scenario is their personal information. It is important to understand the extent to which a person wants himself/herself to be identified in public or chooses not to be identified at all. Ruth Gavison expresses his concern about our accessibility. For example, the extent to which others know us, the degree to which we are accessible to others physically, as well as the extent of attention we desire from others. Our identities and the public persona attached to them take forever to build a positive image, but just a fraction of a second to lose it completely. We share and disclose certain aspects about ourselves with some people. What we choose to make available to people and what they reveal to us influence our interactions with them. Both obscurity and anonymity serve as protective factors. Such anonymity helps in concealing characteristics like gender, race, ethnicity, or class that could influence how others view someone else's work and beliefs. The disclosure of information disintegrates the value of anonymity and violates the right to privacy which is an integral part of a person's life. Furthermore, the dissemination of personal data on any platform without the consent of the data owner infringes the data privacy of the individual. Thus, the breach of data privacy weakens the value of anonymity.

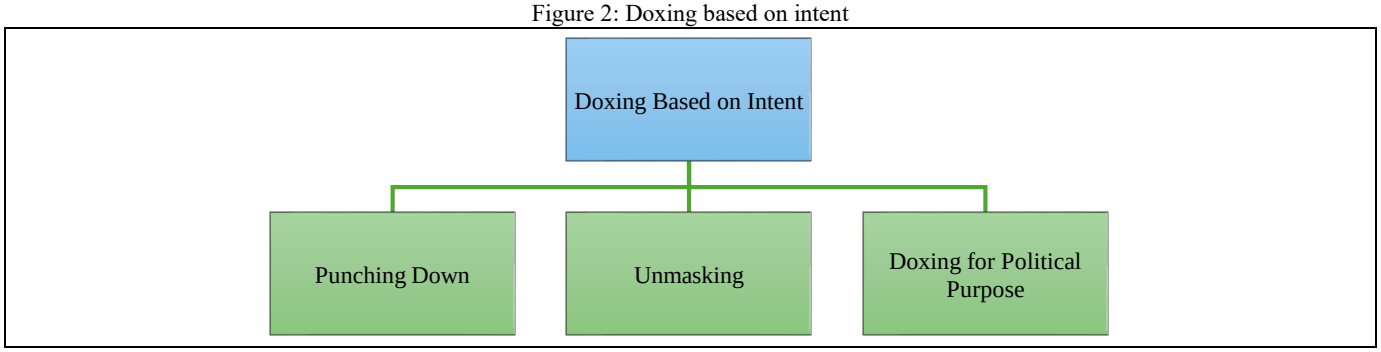
7. Patterns of Doxing:

Figure 1: Patterns of Doxing



Doxing can be classified into different types such as De-anonymization doxing, Targetted Doxing and De-legitimization Doxing. Of all these, *De-anonymization Doxing* is the broad type. Generally, being anonymous denotes that a person doesn't want himself/herself to be identified or disclose his/her details to the world. Also, it may include individuals who use aliases or pseudonyms to keep their identity discreet. Here, such personally identifiable information (email, phone number, etc) about an individual is disclosed without their consent, thereby causing loss of anonymity to the subject. Additionally, it includes instances where, regardless of whether a person has made a conscious effort to keep his/her identity discreet, such a person's details are made public. *Targeted Doxing* discloses information about a person's physical location. Here, the accessibility to an individual gets easier, which increases the degree of vulnerability towards physical harm. Such acts can result in various forms of harassment as well. The loss of obscurity of the victim renders them more susceptible to attacks. The accused may impersonate or make hoax calls to police which is also known as swatting. There was a case where the victim received a pizza which wasn't ordered by her, rather it was under the name of the accused who was charged with murder and was known to the victim.[2] In *De-Legitimization Doxing*, the information is disclosed to shame the victim. It is done to ruin their reputation, character or the social persona they have in society. Due to such disclosure, the credibility of the individual is lost. They are ridiculed and tagged as hypocrites in society. The misogynistic attitude of the perpetrators involves using sexuality as a means to shame the victims. They consider the victims as mere objects. For example, an unmarried girl undergoes an abortion which is considered taboo and stigmatized in many societies, and if the information related to her abortion is circulated, then she might be subjected to criticism, disdain, character assassination and other forms of bullying. Similarly, there have been cases reported where confidential medical records were leaked, leading to online harassment and mockery. Also, there are instances where intimate photographs along with personal information identifying such victims are revealed online by the perpetrators who have been acquaintances of such victims or rivals. Such revelation often leads to unemployment, ostracization from society and many other repercussions that are borne by the victims. According to the intent of the perpetrator, Doxing can be further categorized into three types: Punching Down Doxing, Doxing for Political Purposes, and Unmasking.[3]

Figure 2: Doxing based on intent



Source: Adapted from MacAllister (2017)

[1]Reichel, P. L, 'Dossier building as a social problem topic', [1977], Teaching Sociology, 4(3), 293–306.
[2] Mantilla K, *Gender trolling: How misogyny went viral,* Praeger 2015
[3] Julia M. MacAllister, '*The Doxing Dilemma: Seeking a Remedy for the Malicious Publication of Personal Information*' (2017) 85 Fordham L Rev 2451

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 2309-2315

In the case of Punching Down Doxing, the perpetrator has pure malicious intent like harassment, revenge, enmity, stalking, and bullying. It includes instances such as disclosing personal information, intimate pictures and chats online after a breakup, seeking revenge against the other. Generally, victims are threatened with damage to their personal or professional lives, sometimes including their family members. The prime motto of the perpetrator is to silence the victim of doxing. Therefore, they adopt every possible method and encourage others to harass and bully the victim. Doxing for political purposes is carried out to expose insider information and leak confidential information. One such example is Chelsea Manning, who disclosed thousands of sensitive data related to military and other diplomatic strategies to WikiLeaks in the year 2010. The disclosure in this form of doxing was argued to be non-malicious. Perpetrators claimed such disclosure was done for good cause by exposing the abuse and atrocities by the states. Other cases include doxing by The New York Times, which disclosed a snippet of reports related to the Tax returns of Donald Trump, who was the then-presidential candidate and was believed to have concealed his tax returns during the campaign. Similarly, in the case of Black Lives Matter, the doxers claimed to expose racial discrimination and atrocities inflicted by the police. Thus, it has been difficult to criminalize doxing, especially when perpetrators claim to dox in good faith.

The third type of Doxing, i.e. Unmasking, where in order to maintain internal regulation, the members of the Doxing group reveal the identity of their fellow member who doesn't conform with the regulations of their group anymore and is likely to be a hurdle in the fulfilment of their agenda. For instance, the details of a leader who turned hostile as an FBI informant were disclosed to the administration by the members of the doxing gang to protect themselves from further harm.

8. Effects of Doxing:

Once the information is out on the internet, it doesn't get erased easily. The act of Doxing can have devastating effects on the lives of the victims. For instance,

Mental Health

The degree of mental harm towards the victim always goes unnoticed after an offence. Individuals who are doxed, are subjected to constant criticism, vilification, trolls, ridicule, harassed and therefore face difficulty coping with the situation they are put into. Such acts deeply affect the status of their mental well-being. Such individuals might experience trauma, anxiety, stress or face any other kind of mental health issues. According to research conducted by *Safe Home Organization*, a victim said 'I was up and down, swinging from manic to depressed'. Similarly, another victim of Doxing had to be hospitalized due to deterioration of mental health.[4] These instances highlight the grim reality on how the world stands on the grim of collapse due to misuse of technology.

Financial Loss

There have been many cases where the victims lose money due to identity theft and fraudulent accounts operated by the perpetrators who evade taxes, buy expensive products and scam other people. Thus the victims of Doxing are also at risk of financial harm.

Negative Publicity

Such acts of the perpetrators damage the reputation of victims both on a professional front as well as on a personal basis. As a result, many people lose their jobs. Victims are usually portrayed as hypocrites or a person of loose character, which has a negative impact on their reputation in society. People are ostracized and boycotted from their communities after personal details, which might include intimate details, are disclosed in public. They face humiliation and embarrassment, taking a toll on their psychological health.

Physical Harm

Entering the name of the victim of Doxing on a search engine may reveal their personal information, which could be an easy medium to reach him/her. The accused can also encourage others to abuse the victim, which may increase the risk of physical harm. This act could be equated with sexual harassment on the Internet which includes stalking, bullying, etc. The victims of Doxing report being followed by unknown people to their residences, workplaces, etc. They are under constant surveillance, threatened, intimidated and live in fear of being attacked. The perpetrator may be one person or more than one and sometimes, a mob. This hampers the victim's basic fundamental rights, which include the right to move freely, the right to life and personal liberty, as well as their right to privacy.

9. Case Studies Illustrating Doxing:

In 2024, the plaintiff of a case[5] posted from her 'X' handle (formerly known as Twitter) about the interview of a certain public figure. Due to the difference of opinion, the plaintiff received severe backlash from other users. First, her personal photographs, address, and professional identity were disclosed on X, and then an email was sent to her employee. The Honourable Court directed the tweets and URLs to be taken down and mentioned the nature of Doxing, its effects and the importance of making it a statutory offence. It was of the view that if Doxing remains unchecked, it could violate the Right to Privacy, and relief under the privacy judgement[6] and dis-balance the scales of justice.

Following the above pattern, American Football Coach Dan Campbell in 2024 was a victim of doxing. The personal address of the coach was leaked by his daughter's classmate. The perpetrator uploaded the residential details of Campbell via Snapchat following which the residence was visited by several unknown people hovering around the vicinity of the house. As a result of this, the coach with his family had to relocate to a different place for their safety and security.In another case[7] of Doxing, after the victim broke up with her boyfriend, he created a fake profile in her name on Yahoo! and posted her workplace address, residence address, contact number, objectionable photographs, and nude images that were taken without her permission and consent. Also, by impersonating the victim, the perpetrator invited male persons to have intimate chats. Due to such acts, the victim received indefinite calls and chats which used to be indecent in nature, demanding sexual favors. She also had unknown men at her residential address with the misconception that she consented to sexual advances. She sued Yahoo! for its negligence in not removing the fake profile and obscene material. However, due to the protection of Internet Service Providers under the Communications Decency Act, 1966 the case was dismissed. The video of Amy Cooper was posted online, where it was perceived that she made certain racist comments. After the release of the video, her address, telephone numbers, emails, and workplace address were leaked online. After such disclosure, she received numerous calls, including death threats, abuse and was bullied online. After a few days, hundreds of people gathered to protest in front of her residence, and thereafter, she was fired from the investment firm where she worked at. Thus, she was at a loss in her personal as well as professional life. A Jewish-American lady filed a suit against the creator of a website, "The Daily Stormer", who launched a troll attack against her with more than seven hundred hateful comments, death threats, and demeaning messages[8]. Further, the perpetrator urged his supporters to harass her, including her spouse and child. She faced severe criticism and backlash damaging her reputation in society. Her mental health deteriorated, leading to panic attacks, anxiety and stress. The Court delivered judgment in her favour and directed the accused to compensate the victim with an amount of $14 million to the victim.

---

[4] Max Sheridan, '*Doxing Statistics in 2024: 11 Million Americans have been victimized*', 2024, SafeHome.org
[5] *Shaviya Sharma v Squint Neon & Others* [2024] LNIND1308 (DEL)
[6] *K.S. Puttaswamy v Union Of India*, [2017] 10 SCC 1
[7] *Barnes v Yahoo! Inc* 570 F 3d 1096, 1098
[8] *Gersh v Anglin*, 2019 U.S. Dist. LEXIS 133795 (D. Mont.)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 2309-2315

A harassment campaign was launched in the year 2013, which was known as the GamerGate Campaign. It was carried out by those who opposed the concept of feminism, empowerment, and equality in the video game culture. It targeted women and those who advocated for such rights in the video game industry. Video game developers like Brianna Wu, Anita Sarkeesian, and Zoe Quinn were prime targets.

Zoe Quinn's game was criticized and received backlash from the online gaming industry as it dealt with issues of depression. People didn't like the fact that it deviated from the traditional pattern of gaming culture. Later, a blog was posted by Zoe's ex-boyfriend, who revealed personal details of their relationship, including their chats, messages, videos, etc. Such revelation escalated the hatred amongst the people who carried out the campaign to such an extent that she started receiving hate comments, death threats, and rape threats and was subjected to constant trolls and ridicule. In addition to this, Zoe's personal address was also circulated. Unknown people started visiting her house and threatening her. As a result of these, she had to relocate to a different place for her safety and security.

Similarly, Anita Sarkeesian received the first backlash after her analysis on the YouTube video Tropes vs Women in Video Games where she criticized the sexist portrayal of women in video games. Her opinion wasn't accepted by the misogynistic groups, and therefore, all her personal details, including her address, were circulated online. She received death threats and violent threat messages and had to flee from her residence. In a like manner, Brianna Wu, who tweeted in opposition to the Gamergate campaign, was a victim of doxing by the campaign's supporters. All identifiable information about her was leaked online. She received threats and hateful comments, including mutilated images of dogs. Within six months in 2015, she received forty-eight death threats. She relocated along with her spouse and lived with pseudonyms. The consequences of the harassment were such that she was diagnosed with post-traumatic stress disorder. These cases indicate that doxing is merely an annoyance rather a precursor to consequences in real world. Therefore, in order to comprehend how such actions are penalised or prevented, it is important to examine the legislative framework.

10. Legislations

National Scenario

- *India*

Doxing has not been directly addressed anywhere in the legal landscape of India. There is no statutory offence with respect to it. However, issues relating to Data Privacy, Cyber Security, Cyber crimes, and their punishments are dealt with under the Information Technology Act (IT Act) of 2000. Also, another act was enacted in 2023, known as the Digital Personal Data Protection Act, 2023 which aims to strengthen the data protection system and control the handling of personal data. However, as these laws do not clearly address the malicious revelation of personal information in the context of doxing, these rules continue to be fragmented in nature. This create challenges in the enforcement procedure and makes it difficult for victims to access appropriate remedies.

International Scenario

- *Hong Kong*

The increase in the number of offences relating to doxing led the government of Hong Kong to introduce the Personal Data Privacy Amendment Bill, 2021 which was put into operation as the Personal Data Privacy Amendment Ordinance, 2021. This modification recognized and criminalized offences related to doxing. They categorized "specified harm" into four types. First "specified harm" includes Pestering, causing threats or intimidating the person, molesting, and harassing. The second category includes causing psychological or bodily harm to that person. The third category consists of causing harm to a person such that the person is compelled to be concerned about their safety and security. The last category includes damage to the property of the person concerned.

The amendment also introduced doxing in a two-tier format. The 1st tier constituted under section 64(3A) states that when with the intention of causing "specified harm" the personal information of an individual is revealed without his/her approval and such reckless disclosure is likely to cause any specified harm to the individual or their family, the person who commits such offence will be liable for imprisonment up to two years and fine of HK$100,000 under this section which will be tried summarily.

The 2nd tier includes additional elements of the 1st-tier offence thereby inflicting severe punishment than the first. It is an indictable offence where the offender harms the data subject or his/her family members due to such disclosure. For such an offence, the offender will be punished with imprisonment up to five years and HK$1,000,000. Under the amendment, the Commissioner has been conferred powers relating to investigation and prosecution. It also authorizes the Commissioner to serve notice of cessation to restrict disclosure of Doxing content, and it will be applicable against Hong Kong as well as non-Hong Kong operators.

- *Netherlands*

Under the Dutch Criminal Law, as of January 1, 2024, it is illegal to provide, distribute, or otherwise make personal information public with the goal of intimidating someone.[9] The Dutch Criminal Code (Wetboek van Strafrecht, WvSr) categorises Doxing as a felony, i.e. misdrijf and one who commits such offence will be punishable with two years imprisonment or 4th category fine that is currently maximized till € 22,500. The new section 285 D of the Dutch criminal code mentions Doxing. It states that a maximum period of 2 years imprisonment or fine from the fourth category will be imposed on an individual who acquires personal data about another person or a third party and such individual distributes or makes such information available with the intent to frighten or instil fear to that person, cause nuisance, severely hamper the performance at his place of employment or line of work. Also if such an offence is committed against a person with a specific profession or position as a Lawyer, Police, Minister, Judicial officer, Mayor etc then the prescribed punishment shall be increased by one-third.

- *United States of America*

There are various federal approaches in the United States towards Doxing. Like -

A. "Communication Decency Act, 1966",

B. "The Interstate Communications Statute",

C. "The Interstate Stalking Statute"

Under the first act, transmitting or broadcasting "obscene or indecent" materials to those who are below the age of eighteen years was made illegal. The goals of this act were to encourage unrestricted communication of information and concepts on online platforms and to foster proactive monitoring for objectionable or explicit materials.

Limitations: The addition of the Good Samaritan Law tends to be a hindrance as it protects the service providers from liability. Additionally, Section 230 of the said law protects ISPs and users against accountability for wrongdoing committed by third parties on their online platforms or websites, although the provider does nothing after being aware of the objectionable content.

'Provider or user of an interactive computer service shall not be treated as the publisher or speaker of any information provided by another information content provider'. [10]

[9] Joanne van eenenaam, '*Doxing is a crime under Dutch Criminal Law as of January 1, 2024. What does that mean?*', 2024, WiseMen Advocaten

[10] Communications Act of 1934, s 230(c)(1)

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 2309-2315

The Interstate Communication Statute states - If a conversation contains threats related to kidnapping or injury to an individual and such communication is transmitted, such act is criminalized. The prosecutors can use section 875(c) to charge a person with doxing if there is a combination of such threats with the intent to dox.

Limitations: For the determination of culpability, the Apex Court observed that knowledge of mens rea was enough.[11] Nonetheless, the higher court extended discretion in this case to the lower court for a determination of negligence, which made it difficult to ascertain whether the doxer was confident that his actions would lead to such offense. It was considered to have set high standards, and difficult to prove the act.

Similarly, the definition under this act tends to be strict. It is possible that threat or injury might not be communicated expressly, although it might lead to reasonable apprehension in the mind of the victim. In such a case, if the communication doesn't contain an express mention of threat or injury as mentioned under this act, then the offender will escape from liability.

The use of 'any interactive computer service' in a 'course of conduct' that puts an individual in reasonable fear of death or bodily injury or 'causes substantial emotional distress to a person' is prohibited under the Interstate Stalking Statute. [12]

- *Australia*

The Australian government has laid down a landmark legislation known as The Privacy and Other Legislation Amendment Bill, 2024 on 12th September, 2024.[13] It was noticed that The Privacy Act of 1988 was not able to keep pace with the changing digital world. Thus there was a necessity of introducing a new legislation to meet the demands of society. The new Bill aims to address concerns relating to Children and their privacy, to strengthen Data privacy laws. It also introduces new criminal offences to outlaw doxxing and breach of personal data. The penalty fixed according to the Bill is a maximum of six years imprisonment for misuse of personal data, and a greater punishment of seven years imprisonment when individuals are targeted based on their ethnicity, caste, race, religion, etc.

- *Spain*

Although there is no specific mention of 'Doxing' under federal laws of Spain, there is certain legislation under the purview of which this offence can be addressed. The '*Organic Law 3/2018 on Protection of Personal Data and Guarantee of Digital Rights',* which is in conformity with the General Data Protection Regulation, 2018 of the European Union, deals with laws related to data protection. It consists of 97 articles put together in 10 headings which separately deal with data processors, their liability, data protection mechanism, defaulters lists, and various rights of the data subjects. While Heading 7 deals with the Spanish Data Protection Authorities, Heading 9 outlines a list of transgressions categorized as extremely severe, severe or minor and governs the legal penalties for infringing the law.

Additionally, the Spanish Criminal Code established by the Organic law 10/1995, under section 197-201 penalizes those who intrude into the privacy of an individual without their consent, capture any of their documents, messages, photos, emails etc shall be punished with imprisonment up to 4years and fine. Furthermore, the amendment of 2015 states that those who circulate the above-mentioned data to third parties shall face imprisonment of 2 years to 5 years and a fine of 12-24 months.

- *South Korea*

South Korea is one of the few nations with a code that expressly tackles doxing. The Act on Promotion of Information and Communications Network Utilization and Information Protection, Act No. 14080, Mar. 22, 2016, expressly provides under Article 44, which restricts users from disseminating any content through communication and information networks about an individual that violates their rights, intrudes into their privacy and is likely to be defamatory. Also, the service providers must ensure the protection and prevention of information from being circulated through their network. Additionally, there is the Korean Communications Commission, which may prepare a plan of action for protecting the rights of individuals and make policies to prevent the circulation of data through communication networks.

Whenever there is a breach of privacy, the aggrieved person can request the service provider to delete the information that has been circulated through their network or ask for a rebuttal statement. On such request, the service provider shall delete the information or issue such statement of rebuttal. The service provider also has the authority to temporarily block access to such information when they find any dispute between the interested parties. Additionally, under Article 44(3) temporary discretionary powers have been conferred upon the service providers, where if a violation of someone's privacy through their network comes to the knowledge of the service providers, then they can take measures to restrict further circulation of such information and take necessary steps.

Article 49 of the above act states that any information that is processed or available online about a person should not be altered or misused by anyone. In fact, no one should try to steal or reveal confidential information about any person. On receiving a report from a service provider with respect to a breach of such privacy and defamation, the Ministry of Science (ICT) the Korean Communication Commission or Korean Internet and Security Agency shall take relevant measures to tackle the issue.

Furthermore, the "*Personal Information Protection Act*" which came into effect on 1st January 2004, has been brought to protect the data of common citizens, regulate the processing of data and proper usage, etc.

11. Findings:

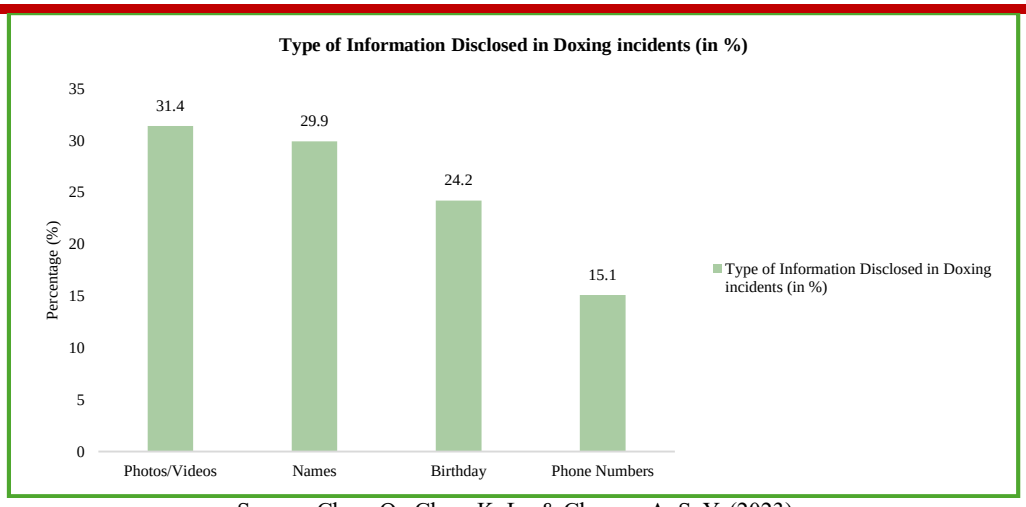
The study reveals that the harm caused by doxing extends beyond conventional privacy violations. It seems to be multifaceted in nature, affecting mental well-being, reputation, financial stability and the safety of people. Even when the data is public, the intentional act of accumulating and disseminating it to go after a particular person converts information into an instrument of violence, stripping away their right to privacy and individual autonomy.

A study by Chen et al. (2018) outlines the categories of personal information revealed in doxing incidents (Figure 3). The results indicated a sizeable percentage of victims claimed being exposed to sensitive information, which included personal images or videos (31.4%), names (29.9%), birthdays (24.2%), phone numbers (15.1%). These data indicated that personally identifiable information was likely to be most targeted, raising the potential risk of harassment. These results also highlighted the easy availability and accessibility of personal information online.

Figure 3: Type of Information Disclosed in Doxing incidents (in %)

[11] *Elonis v United States*, 135 S. Ct. 2001, 2004 (2015)
[12] 18 U.S.C. S 226(1A)(2)(A) -(B) (2012)
[13] The Hon Mark Dreyfus KC MP, '*Better Protection of Australian's Privacy*', 2024 <https://ministers.ag.gov.au/media-centre/better-protection-australians-privacy-12-09-2024>

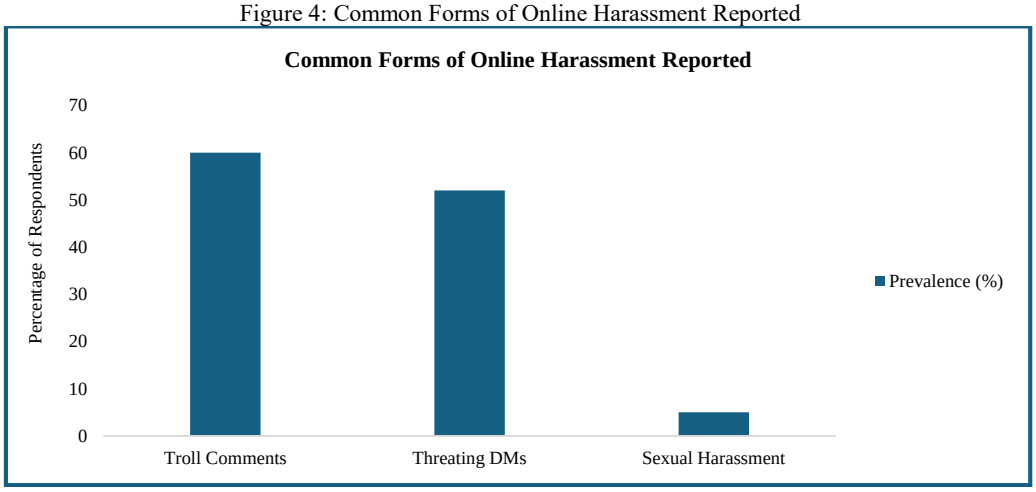
MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 2309-2315



Source: Chen, Q., Chan, K. L., & Cheung, A. S. Y. (2023)

The ubiquitous nature of trolling and public shaming seems to catalyze an evolving crisis towards weaponising personal data in the digital era. The survey conducted by Amnesty International in 2024 indicated 52% of the participants received threat messages on their DMs (Direct Message), and 60% of the participants alleged disrespectful trolling (Figure 4). Such widespread trolling and shaming highlights the dual-layered threat, which integrates public humiliation and private intimidation. Furthermore, 5% incidents of sexual harassment, including non-consensual images generated by Artificial Intelligence, reflect a potentially dangerous shift taking place due to technology, which might be used to dehumanize people.

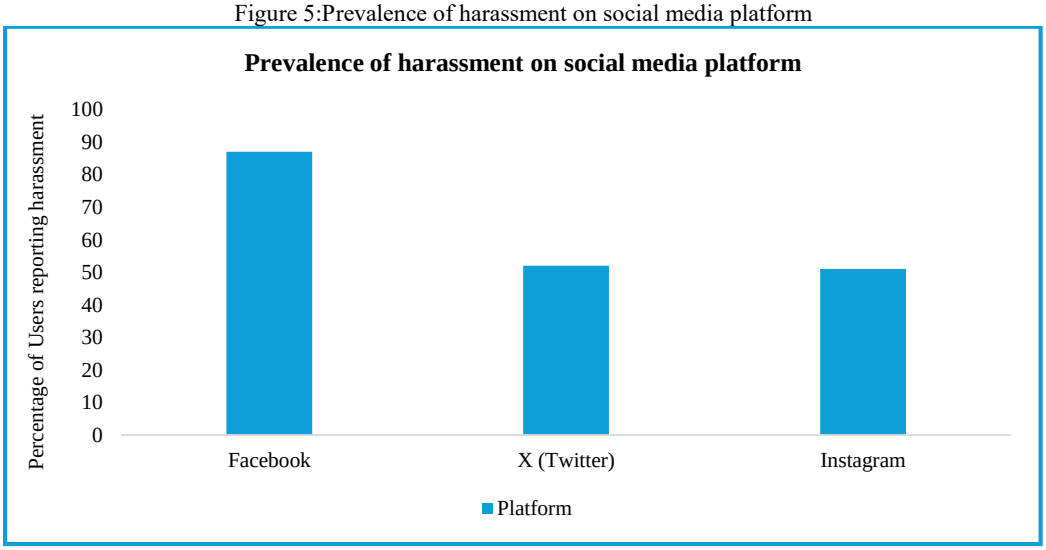
Figure 4: Common Forms of Online Harassment Reported



Source: Adapted from Amnesty International Global Campaign, 2024

Another survey conducted by Amnesty International in 2024 revealed a glaring gap in security across social media platforms. It was noted that 87% of the users who were harassed reported Facebook as the most toxic and hostile online setting (Figure 5). It had the highest percentage of reported cases of harassment as compared to X and Instagram. This implies that the content control mechanisms and privacy settings implemented on big online social media platforms fail to take sufficient measures to combat such persistent digital violence. Figure 5 below indicates which social media platform has the highest number of reported cases of harassment.

Figure 5:Prevalence of harassment on social media platform



Source: Adapted from Amnesty International Global Campaign, 2024

MSW MANAGEMENT -Multidisciplinary, Scientific Work and Management Journal
ISSN: 1053-7899
Vol. 36 Issue 1s, 2026, Pages: 2309-2315

The analysis of case studies draws attention to the serious and irrevocable repercussions faced by the victims such as social rejection, threats, harassment and exclusion in personal and professional life. These incidents highlight how doxing can escalate from just being a social media exposure to physical stalking and crime in the real world. This study also reveals the inadequacy of legal remedies as victims find it challenging to hold the perpetrators accountable for the crime. Furthermore, the study reveals that current legal framework in India is disjointed and lacks specific acknowledgement of this problem leading to doctrinal ambiguity and insufficient remedies. Conversely, comparative analysis indicates that nations with explicit legal provisions relating to doxing have clear standards of liability that grant effective protection and facilitate expedite legal redress to the victims, underscoring the need for a cogent and thorough legislative approach in India.

12. Suggestions and Recommendations:

Need for Stringent Legislative Provisions: As the information circulated online has a varying degree of publicity, Doxing needs to be addressed with a clear and precise definition. This is required because generally, the doxers escape liability by stating the prior availability of information online. Also, there have been circumstances where personally identifiable information is easily available on the internet or where individuals upload their information themselves at their own will. In such cases, there is a requirement of distinction between the ingredients which amounts to doxing and which doesn't. Law enforcement authorities should take steps to criminalize Doxing as an offence in all countries. Strict action must be taken against the malicious publication of information.

Extending Support to the victims through a proper mechanism : Generally, the victims of Doxing undergo media trials and societal shaming, ultimately affecting their mental and physical health. Therefore, there should be enough support networks for victims of Doxing which could help them to recover from the mental stress and trauma they go through due to such acts. It may be in the form of counselling, legal assistance and moral support.

Awareness Programme : In addition to these, Awareness Campaigns are a must for changing the perception of society. Workshops can be conducted to promote digital literacy among individuals to protect their personal data over online platforms. There must be programs educating people about their rights and procedures to seek justice. The culture of responsible online behaviour must be cultivated among the youth.

*Need for IT support for identification and monitoring Doxing cases.*Generally, the accused escapes liability when there is a tussle between Internet Service Providers and victims which poses a hurdle in the path of justice. Therefore, collaboration with the IT sector could help in the early detection of Doxing cases and monitor Doxing content. The technical teams can help in removing the personal information circulated online thereby preventing further circulation of data. Additionally, they can develop algorithms for the erasure of victims' data that is released online, without their consent. These steps can also help in safeguarding the right to be forgotten of a victim. Thus, a techno-legal collaborative approach might help the authorities to function efficiently in matters related to Doxing.

13. Conclusion

A particular act can have a wide range of potential outcomes. On the contrary, the laws pertaining to such conduct tend to be limited. Thus, the scope of that act is sometimes overlooked. It is crucial to comprehend the nuances of doxing, the severity of harm it can cause and the justifications for criminalizing it. Doxing can have detrimental effects on both the victim and society. In the present scenario, the value of anonymity needs special attention. The dissemination of personal information, as in the case of doxing of an individual invades his/her privacy as well as the right to have a safe and secure environment. Although there have been several judgments emphasizing the necessity of protecting the privacy of an individual, by laying down new privacy laws, such laws need to be appropriately enforced. As a result, the reliability on general laws will decrease, and the complications due to doxing can be tackled with concrete laws, thereby saving the time of courts and individuals. Therefore, there is a need for a flexible approach to solve this issue. In summation, a culture of responsible individuals and a secure online environment can be promoted to reduce the risk of Doxing by combining awareness, digital literacy, technical assistance, legal recourse and community support.

References

1. Amnesty International. (2024, July 1). *Three out of five young activists face online harassment globally for posting human rights content*.
2. Barnes v Yahoo! Inc 570 F 3d 1096, 1098.
3. Chen, Q., Chan, K. L., & Cheung, A. S. Y. (2018). *Doxing victimization and emotional problems among secondary school students in Hong Kong*. International Journal of Environmental Research and Public Health, 15(12), 2665.
4. Communications Act of 1934, s 230(c)(1).
5. Dreyfus M. Better protection of Australians' privacy [Internet]. 2024 [cited 2025 Nov 10]. https://ministers.ag.gov.au/media-centre/better-protection-australians-privacy-12-09-2024
6. Douglas, D.M. Doxing: a conceptual analysis. *Ethics Inf Technol* 18, 199–210 (2016). https://doi.org/10.1007/s10676-016-9406-0.
7. Elonis v United States 135 S Ct 2001, 2004 (2015).
8. Gersh v Anglin 2019 U.S. Dist. LEXIS 133795 (D Mont).
9. S. Puttaswamy v Union of India [2017] 10 SCC 1.
10. **Kukul, B. (2023).** Personal data and personal safety: Re-examining the limits of public data in the context of doxing. *International Data Privacy Law, 13*(3), 182–193. https://doi.org/10.1093/idpl/ipad011.
11. Mantilla K. *Gender Trolling: How Misogyny Went Viral*. Santa Barbara (CA): Praeger; 2015.
12. MacAllister JM. The doxing dilemma: Seeking a remedy for the malicious publication of personal information. *Fordham Law Review*. 2017;85:2451–2483.
13. Meyer, S. (2024). *Doxing in cyber security: A full guide*. Moxso. https://moxso.com/blog/glossary/doxing
14. Pratama, A. R., & Sari, N. K. (2024). Digital Privacy and the Legal Challenges of Doxing: A Comparative Perspective. *Proceedings of the International Conference on Reform of Turkish Law (ICRTLaw)*, 1(1).
15. **PEN America,** *Shouting into the Void: Why Reporting Abuse to Social Media Platforms Is So Hard and How to Fix It* (2023)
16. Reichel PL. Dossier building as a social problem topic. *Teaching Sociology*. 1977;4(3):293–306.
17. Shaviya Sharma v Squint Neon & Others [2024] LNIND 1308 (Del).
18. Sheridan M. Doxing statistics in 2024: 11 million Americans have been victimized. *SafeHome.org*. 2024.
19. Van Eenenaam J. Doxing is a crime under Dutch criminal law as of January 1, 2024: What does that mean? *WiseMen Advocaten*. 2024.
20. 18 U.S.C. §226(1A)(2)(A)-(B) (2012).