Doxxing Celebrities: Addressing Legal Gaps and Proposing Reforms in India

Nihitha PK
Student
Department of Law
Sastra Deemed to Be University, India

Abstract — The visibility of well-known figures like celebrities and social media influencers has drastically increased due to the increase usage of social media platforms, thus making them susceptible to online harassment and doxxing. Doxxing entails exposing personal information about individuals without their consent, mostly with an aim of intimidating or harassing them through unwanted attention, threats or physical harm. Despite its increasing rate, particularly among celebrities, there are no regulatory frameworks designed to combat doxxing in India. This absence emphasises serious legal issues regarding privacy rights and cyberbullying. This article examines the applicability of existing provisions on cybercrime law, privacy laws and defamation laws in major jurisdictions worldwide. After identifying the legal gaps, the researcher proposes specific changes that will help define doxxing more clearly and strengthen the legal framework aimed at protecting individuals from such assault on privacy.

Keywords: Doxxing, Celebrities, Privacy, Online Safety, Legal Framework

I. Introduction

The rapid evolution of the digital era has led to transformation of the way in which people communicate with each other, and also increase in the misconducts happening online such as cyber harassment and doxxing/outing. The term ‘Doxxing' is short for ‘dropping dox', (‘dox' is a slang word for ‘Documents’). In simple words it is the act of revealing personal information about someone online. Prior to the predominant use of the internet, the act of disclosing personal details without ratification was not new, but the term 'doxxing' didn’t come into use until 1990s. During this period, anonymity was greatly prized. Conflicts between rival hackers sometimes reached a level where one would 'drop docs' on another, disclosing personal details about someone who was previously known only by their username or alias. Initially, the term 'doxxing' was used to unmask hidden online identities. However, its meaning has since expanded beyond hacker communities to include the exposure of personal information about individuals who reveal their true identities on social media platforms such as Instagram, X (formerly Twitter), and Facebook.

When personal information of a person such as home addresses, phone numbers, or private schedules is maliciously spread online, they face heightened security risks as well as physical threats. The impact of doxxing on celebrities is particularly severe as they are already navigating through the challenges of living in public eye. Famous celebrities are often being the victims of such acts due to their greater visibility, success, and the public’s fascination with their personal lives. The sudden loss of privacy can cause emotional distress, as celebrities often find themselves and their loved ones under increased surveillance or facing direct threats. It can even disrupt their professional lives, as security concerns may lead to limited interactions with fans, ultimately affecting their careers and reputations. All the more reasons for doxxing to become a criminal offence in India.

In India, there are existing laws which addresses doxxing related issues such as voyeurism (Section 77, BNS and Section 66E, IT Act), divulging sexually explicit content (The IT Act) and obscene content (Section 294 BNS), defamation (Section 356 BNS) and online stalking (Section 78 BNS). Doxxing violates our Right to Privacy (Fundamental Right) and threatens our Right to Dignity (Article 21 of the Indian Constitution), and subjects us to harassment and places us in danger directly. The absence of anti-doxxing laws in India highlights a significant gap in the country’s legal framework when it comes to addressing the growing issue of online privacy violations.

II. Objective of the Study

The objective of this article is

- to analyse the increasing frequency of doxxing, particularly its impact on high-profile individuals such as celebrities and social media influencers, and
- to highlight the inadequacies in India’s current legal framework to address this issue.
- to explore existing cybercrime, privacy, and defamation laws in major jurisdictions worldwide, identify the gaps in India’s legal protections against doxxing, and propose legislative changes that will clearly define doxxing and enhance legal safeguards for individuals against such privacy violations.

III. Literature Review

Doxxing, the malicious practice of revealing an individual's private or identifying information online without their consent, has emerged as a significant threat to the privacy and security of individuals, particularly celebrities. Current legal frameworks, including data privacy laws like the GDPR, partially address this issue but fall short. The GDPR’s “right to be forgotten” is limited to cases of inaccurate or excessive data, while Germany’s NetzDG mandates content removal only if it’s clearly illegal, not specifically targeting doxxing. These limitations hinder effective action against doxxing. To address this, new legislation should treat even a single doxxing incident as punishable if malicious intent is evident, as proving a pattern of conduct can be challenging. Social media platforms also have a vital role in prevention, employing AI-based tools to detect and promptly remove doxxing content. A combined approach-strengthening laws against doxxing while implementing protective measures on

digital platforms-is essential to safeguard individual privacy and security in today's online environment.

The authors view doxxing as a serious online abuse with significant repercussions, including harassment and potential physical danger. They note that while doxxing is technically simple, it causes lasting harm, affecting diverse individuals for personal, competitive, or political reasons. Aiming to address limitations in previous research, the authors take a quantitative approach to measure the scale, frequency, and impact of doxxing. Their findings reveal that doxxing often leads to social media account closures, and they propose tools to notify potential victims and inform authorities to mitigate risks.

"Wielding Power and Doxxing Data" examines how personal information can be weaponized online through doxxing, impacting the regulation and control of individuals' digital identities. Hutchinson suggests that doxxing, by revealing private information, disrupts personal autonomy, effectively controlling how people interact online and shaping their digital self-representation. The chapter discusses doxxing as a powerful tool, highlighting its implications on privacy and the broader influence of digital surveillance on personal freedom.

IV. GROWING TRENDS OF DOXXING:

In Indian society, celebrities and influencers hold a unique and revered position, with many people regarding them as role models. This admiration often fosters an unhealthy level of curiosity about their personal lives, which is further amplified by doxxing. High-profile individuals frequently use social media platforms like Instagram, Facebook, X (formerly Twitter), and YouTube to engage with their followers, sharing glimpses of their daily lives, activities, and locations. While such engagement is essential for maintaining a connection with fans, it inadvertently creates a digital trail that doxxers can exploit. In some cases, information posted online has been used to track and monitor the whereabouts of celebrities, leading to serious invasions of privacy and even physical security risks.

A. Impact on Privacy, Personal Boundaries, and Psychological Well-being:

The breach of personal boundaries through doxxing can cause immense reputational damage to high-profile figures. With personal information exposed, these individuals become vulnerable to harassment, online trolling, and negative publicity, which can impact their public image and relationships with followers. Many celebrities and influencers face severe emotional distress due to the constant scrutiny and fear of being monitored or confronted. This anxiety often drives them to alter their public interactions, restrict what they share, or even reduce their presence on social media, straining their relationships with fans and affecting their careers. The psychological toll of doxxing extends beyond public image concerns, deeply impacting mental health. Victims often experience chronic stress, anxiety, and depression as they grapple with the fear of intrusion and potential harm to themselves and their loved ones. The constant state of vigilance and insecurity, combined with limited legal recourse in India, leaves many feeling isolated, helpless, and vulnerable. Additionally, the lack of control over one's personal information leads to a sense of disempowerment, as individuals realize they cannot fully protect themselves from digital threats. The combination of reputational harm, emotional distress, and a weakened sense of personal security creates a heavy psychological burden, affecting not only their mental well-being but also their professional engagements and overall quality of life.

B. Public Perception and Ethical Considerations:

Public perception of doxxing in India is complex and often divided, especially when it involves high-profile individuals like celebrities and influencers. Some people view doxxing as a consequence of fame, assuming that public figures, by sharing parts of their lives online, invite scrutiny into their private lives. This perspective, however, overlooks a key ethical concern: "The right to privacy" . Regardless of their public status, celebrities and influencers retain a fundamental right to personal security and autonomy. Doxxing violates these rights, crossing boundaries by exposing private information to the public, which can lead to harassment, reputational harm, and even physical threats. The notion that public figures should "accept" this level of intrusion risks normalizing such harmful behaviour, creating a culture of disregard for privacy and consent.

Ethically, doxxing represents a violation of autonomy, stripping individuals of control over their personal information. It also has a ripple effect on broader online culture, fostering an environment where personal information is weaponized to silence or intimidate. Social media platforms, which enable much of this public interaction, bear a responsibility to curb doxxing by implementing stricter content moderation and privacy protections. When doxxing incidents are left unchecked, they threaten the safety of high-profile individuals and erode the sense of security for all online users. Recognizing the ethical implications of doxxing is essential to fostering a digital space that respects individual rights and promotes responsible behaviour across the online community.

For instance, in February 2024, a woman reached out to the Mumbai Police on X (formerly Twitter) to report a man who had shared a video of her dancing at an event, comparing her performance to sex work. Despite her efforts to address the situation, including locking her account and appealing to the platform, the initial poster refused to acknowledge the harm caused and others shared it and made derogatory remarks to harass her further. While the video was eventually disabled on copyright grounds, it highlighted the growing disregard for privacy and exemplifies the larger issue of doxxing and its consequences.

While fame does bring public attention, it does not negate the right to privacy and autonomy. Doxxing normalizes harmful behaviours, eroding trust in online platforms and fostering an environment where personal information is weaponized against individuals. A collective effort is required to combat this growing issue, involving stricter laws, better privacy protections on digital platforms, and increased public awareness about the ethical implications of violating personal boundaries. By fostering a culture of accountability and respect for privacy, society can work

toward creating a safer and more equitable online space for everyone.

V. CONCEPTUAL FRAMEWORK

A. *Doxxing related laws in India:*

Though there are no existing laws in India to punish and/or address the issue of doxxing, one can attract the following provisions

1) Constitution of India, 1950

The Fundamental Right of 'Right to Privacy and Right to Dignity under Article 21 of the Indian Constitution protects the right to life and personal liberty of every citizen and person, including foreigners. It states that no one can be deprived of their life or liberty without following the due process of law.' This right underpins our freedom to live without interference in our private lives, a freedom that doxxing blatantly violates. Yet, these protections are broad and don't directly address the realities of online harassment .

2) Information Technology Act, 2000

The Information Technology Act, 2000 (ITA 2000) is a crucial piece of legislation that lays the foundation for regulating online activities and safeguarding privacy in the digital space. However, despite its significance, the Act leaves some gaps, especially when it comes to addressing raising issues like doxxing.

Sections 43, 66E, and 72A of the IT Act can be made applicable to elements of doxxing, as they address unauthorized access to personal data, violations of privacy, and the disclosure of private information without consent. Section 43 penalizes unauthorized data access , Section 66E protects against the sharing of intimate images without consent , and Section 72A holds individuals or intermediaries accountable for disclosing personal information in breach of confidentiality agreements.

Despite these protections, the IT Act falls short in tackling specific issues like doxxing, as it lacks clear definitions and tailored punishments. This limitation makes it challenging to hold individuals accountable for maliciously revealing personal details online. For a more comprehensive legal framework, it is essential for the Act to evolve, addressing the specific nuances of digital harassment, including doxxing.

3) Bharatiya Nyaya Sanhita (BNS), 2024

Sections 77, 356, and 78 of the BNS are applicable to certain aspects of doxxing. Section 77 penalizes the unauthorized observation or recording of images in private spaces, which could be used in doxxing to exploit private content . Section 356 addresses defamation, which is often a key element of doxxing, as it involves the intentional harm of a person's reputation through the publication of personal information . Section 78 deals with stalking, which can involve the persistent monitoring and harassment that is typical in doxxing cases . While these provisions can be applied to certain aspects of doxxing, the BNS does not offer a clear, standalone definition of doxxing. As such, the legal framework is limited in addressing the full range of privacy violations that occur online, particularly when personal information is deliberately exposed to harm an individual's reputation or safety.

4) Digital Personal Data Protection Act. 2023

The recently passed Digital Personal Data Protection Act 2023 in India has attracted considerable attention as a pivotal law designed to protect individuals' personal data in the digital era. Although the Act has been approved, it has not yet been officially enforced, leaving many awaiting its implementation and the changes it will bring to data privacy practices across the country. Although it addresses data security, it doesn't specifically tackle doxxing or the kind of individual-to-individual harassment doxxing often involves . However, its provisions address issues related to data misuse and protection that could be applicable in cases of doxxing. Key sections that may relate to doxxing include:

- Obligations of Data Fiduciaries (Sections 6,7 & 8): Fiduciaries (entities processing data) are required to ensure the security of personal data and to process it only for legitimate purposes. Unlawful disclosure of data, such as through doxxing, would likely violate these obligations.
- Grievance Redressal Mechanisms (Section 10): Data principals can approach data fiduciaries or the Data Protection Board of India (DPBI) for grievances regarding breaches, such as unauthorized disclosure of personal data.
- Right to Correction and Erasure (Section 13): The Act grants data principals the right to request the correction or erasure of their personal data when it is no longer necessary for the purpose for which it was collected, or when it is inaccurate. In doxxing situations, this provision can help victims remove sensitive information shared without their consent.
- Penalties for Non-Compliance (Section 30): The Act imposes significant penalties for breaches of data protection obligations, which could apply in scenarios of doxxing facilitated by negligence or malicious intent.

Though the DPDPA addresses data protection and security, it notably fails to tackle doxxing or individual-to-individual harassment. While it includes provisions on data misuse and unauthorized disclosure, these remain insufficient for addressing the malicious and targeted nature of doxxing. Without explicit measures against such personal attacks, the Act leaves a significant gap in safeguarding individuals from this form of digital harassment. The lack of targeted provisions on doxxing raises concerns about the adequacy of the law in preventing and addressing this growing issue.

B. *Role of Judiciary*

Though there is a presence of statutes, it is the role of the judiciary to interpret such legislations and has the potential to fill any loopholes that might be prevalent. Some of the cases that are related to doxxing are discussed below:

1) Shreya Singhal v. Union of India, 2015

The Shreya Singhal v. Union of India (2015) case, which struck down Section 66A of the IT Act for violating free speech, indirectly impacts doxxing crimes. While the decision safeguarded online expression, it created a gap in regulating harmful behaviour like doxxing. Doxxing often hides behind free speech but involves malicious disclosure of personal information. The case highlights the need for targeted legal provisions to balance free expression with protection against privacy violations and online harassment.

2) Shibani Barik v. the State of Odisha, 2020

In this case the Court observed that cyberbullying was on the rise through online platform such as Tik Tok and it emphasized the importance of strict regulation to protect the youngsters and children from being bullied. The Court found that: "the effective government has social accountability to impose reasonable burdensome regulations on the companies that are proliferating such applications, and the appropriate government should do so. Though there is Information Technology Act, 2000 that imposes a responsibility on such companies to remove content and exercise caution before posting any content, India lacks a specialized regulatory framework to address crimes related to cyberbullying.

3) Shaviya Sharma v. Squint Neon, 2024

The case centered on a tweet posted by the plaintiff on X (formerly Twitter) regarding an interview with a politician. Despite the plaintiff's claim of relative obscurity, several offensive responses appeared on social media, including the sharing of her personal information and contacting her employer. The plaintiff alleged that these actions by the defendants amounted to doxxing. The plaintiff's counsel argued that individuals have the right to control their personal information and image, citing legal precedents like Swami Ramdev v. Juggernaut Books Pvt. Ltd., 2018 and K.S. Puttuswamy v. Union of India, 2017 to strong their case. The plaintiff expressed regret over the original tweet and emphasized their intention to stop such behaviour. The Court noted that while the plaintiff's tweet wasn't entirely anonymous, as some identifiable details were available, the subsequent offensive posts and actions were considered aggravating. As a result, the court ordered the removal of the offensive tweets, disclosure of the subscribers' information from Twitter, and details of a Gmail account. These actions were intended to protect the plaintiff's privacy and reputation. The Court acknowledged the growing issue of doxxing and emphasized the need to balance privacy rights with digital data access. Although doxxing is not explicitly defined under Indian law, the court affirmed that it could still infringe on privacy rights, and suggested applying tort and privacy laws for remedies.

4) Scarlett Johansson and other celebrities

Between November 2010 and October 2011, hacker Christopher Chaney gathered information on celebrities like Scarlett Johansson, Mila Kunis and Christina Aguilera from their personal emails, including nude photos and private emails. In a final release, he forwarded all information to two celebrity websites, which, in turn, made everything public. This attack is somewhat unique among doxes in that the perpetrator was identified and sentenced to time in court (10 years, in Chaney's case). As such, his methods were revealed and made public. After obtaining the celebrities emails (presumably through wiretaps and/or 9 network sniffing), he used the "Forgot your password?" link to answer each celebrity's security questions using publicly available information on the internet.

VI. DOXXING LAWS IN OTHER COUNTRIES:

Doxxing laws vary globally, with some countries imposing strict regulations to protect individuals' privacy. Compared to India, where legal frameworks remain limited, other nations prioritize stringent anti-doxxing measures.

A. United States of America:

1) Interstate Doxxing Prevention Act,2000

This Bill modifies the federal criminal code to criminalize the use of mail or any interstate commerce method to intentionally publish, or attempt or conspire to publish, someone's personal information with the intent to bully, intimidate, harass, or stalk. If this action causes the person to reasonably fear death or serious harm to themselves, their family, or intimate partner, the offender faces criminal penalties, including fines, imprisonment for up to five years, or both, along with potential civil liability .

B. United Kingdom:

1) The Data Protection Act.

In order to legally identify any person online you must have a court order issued to the isp of
the person signed by a judge. You cannot use services online to obtain information held on a person without the persons permission hence The Data Protection Act .

2) Protection from Harassment Act,1997

Section 1 of this Act provides that it is an offense for a person to engage in a conduct that constitutes harassment of another, knowing or having reasonable grounds to know that their actions amount to harassment.

3) Malicious Communications Act,1988

Section 1 of this Act specifies that it is an offense for a person to send an indecent or grossly offensive letter or article, whether physical or electronic. The provision has been broadened to cover cases often referred to as 'revenge porn,' making it illegal to share private sexual photos or videos without the consent of the person depicted, with the intent to cause them distress.

4) Communications Act, 2003

Section 127 of this Act states that a person commits an offense if they send, via a public electronic communications network (including the Internet), a message or material that is grossly offensive, indecent, obscene, or menacing in nature, or if they cause such a message or material to be sent.

5) Computer Misuse Act, 1990

This Act contains several key sections addressing doxxing as a form of cybercrime. Section 1, addresses unauthorized access to computer material, defining it as causing a computer to perform any action with the intention of accessing programs or data stored on that computer. Section 2, focuses on unauthorized access with the intention to commit or facilitate further offenses. Section 3, relates to unauthorized actions intended to impair, or done recklessly with regard to impairing, the operation of a computer or similar systems. Section 4, covers unauthorized acts that cause or create a risk of serious damage. Additionally, the Education Act, 2011 grants teachers the authority to search and seize electronic devices and to delete inappropriate images or data.

C. Singapore:

1) Protection from Harassment Act (POHA), 1997

Section 3 of the amended Protection from Harassment Act (POHA) states that an individual will be deemed guilty of an offense if they publish personal information about another

person or a relative of that person with the intent to cause harassment, alarm, or distress, and if the individual indeed experiences such harassment, alarm, or distress. Section 5 of the amended Protection from Harassment Act (POHA) specifies that a person will be considered guilty of an offense if they publish personal information about another individual or their relative, knowing or having reasonable grounds to believe that this could result in unlawful violence against that person or someone else. This Section also states that an individual will also be guilty of an offense if they publish the personal information of another person or their relatives, with the intention, knowledge, or reasonable belief that it is likely to encourage the use of unlawful violence against that individual or anyone else.

D. Australia:

In 2024, Australia announced plans for anti-doxxing legislation following an anti-Semitic incident in which the personal details of over 600 Jewish Australians from a WhatsApp group were leaked, leading to threats. Prime Minister Anthony Albanese emphasized the need to protect the Jewish community, instructing the attorney general to strengthen hate speech laws. The proposed law includes penalties like jail time for doxxing, receiving bipartisan support.

E. Mainland China:

Since March 1, 2020, China's "Regulations on the Ecological Governance of Online Information Content" prohibits online violence, doxxing, deepfake creation, data fraud, and other unlawful activities for online platforms and users.

F. Hong Kong:

As of 2021, doxxing is a criminal offense in Hong Kong, defined as the release of private or non-public information to threaten, intimidate, harass, or cause psychological harm. Convictions carry a penalty of up to five years' imprisonment and a fine of US$128,324.40.

G. Netherlands:

Due to increasing doxxing incidents targeting activists, politicians, and journalists, the Netherlands introduced a law in 2021, making it illegal to share personal data with intent to intimidate or harass . Violators face up to two years in prison or a fine of €25,750 (US$28,204), with enhanced penalties for targeting public figures. The law took effect on January 1, 2024.

H. Russia:

Under Article 137 on "Invasion of Personal Privacy," Russia criminalizes the public sharing of personal information via mass media, the internet, or public events. Offenders face penalties like fines, labor sentences, or up to two years' imprisonment, with additional restrictions on certain positions or activities.

I. South Korea:

South Korea's Article 49 of the "Act on Promotion of Information and Communications Network Utilization and Information Protection" prohibits the unlawful collection and sharing of identifying private information. Despite this law, prosecutions often fall under Article 44, which addresses defamation and derogatory language, often applied in doxxing cases, given its stricter penalties due to the impact of cyberbullying.

J. Spain:

Spain's Criminal Code outlines penalties for privacy violations in Articles 197-201. Article 197, for instance, criminalizes unauthorized seizure of personal data, intercepted communications, and disclosure of private information, with penalties ranging from one to five years' imprisonment, particularly severe when involving minors, economic motives, or sensitive data such as health and religious beliefs.

VII. Suggestions and Recommendations

Based on the analysis of this research article regarding doxxing and its implications, here are some suggestions and recommendations:

- To establish anti-doxxing laws that clearly define doxxing and to establish punishments for individuals who engage in this behaviour. This legislation should outline the purpose behind doxxing, the types of information that can be shared, and the punishments for violators.
- To amend existing privacy laws, such as the Information Technology Act,2000 and the Digital Personal Data Protection Act,2023 to explicitly include protections against doxxing. This can provide a clearer legal structure for injured parties seeking remedies.
- To launch educational campaigns to educate the general public about the dangers and implications of doxxing. This can empower individuals to protect their personal information online and discourage potential offenders.
- To improve the reporting systems for cybercrimes, including doxxing, by creating user-friendly platforms for victims to report incidents easily. This would encourage quicker responses from law enforcement agencies.
- To establish victim support initiatives for doxxing, including legal assistance, counselling, and security measures to ensure their safety. Providing resources can help reduce the psychological and physiological impacts of such incidents.
- To conduct in-depth study to understand the existence and impact of doxxing in India. Data collected can help inform policy resolutions and highlight the priority of addressing this issue.
- To engage in international alliances to tackle doxxing, sharing best practices and team up with other countries to create a unified approach to combat online harassment and privacy violations.
- To encourage the judiciary to interpret existing laws in a way that considers the intricacies of doxxing, ensuring that courts recognize the implications of privacy violations in the digital era and provide appropriate redressals for victims.
- To establish a system for constant reviewing and updating of laws related to cybercrime and privacy to keep pace with technological advancements and emerging threats.

VIII. Conclusion

To effectively tackle the evolving challenges of cyberspace, India must adopt a proactive and specialized approach to its cyber laws. While existing legal frameworks provide a foundation, the unique nature of cybercrimes like cyberbullying and doxxing necessitates tailored legislation to address their complexities and consequences. A comprehensive legal overhaul, combined with robust enforcement, public awareness, and collaboration with digital platforms, is essential to protect individuals in the digital age. By prioritizing privacy, security, and justice in the online realm, India can create a safer cyberspace that upholds the rights of its citizens, safeguards public figures, and adapts to technological advancements. Such measures will ensure that India's legal system evolves alongside the digital landscape, fostering trust and accountability in a rapidly changing world.

References

[1] Doxxing, Wikipedia, https://en.wikipedia.org/wiki/Doxxing (last visited Nov. 19, 2024).
[2] Saurojit Barua, Understanding Doxxing and Its Impact, Mondaq (Apr. 17, 2024), https://www.mondaq.com/india/privacy-protection/1450880/understanding-doxxing-its-impact (last visited Nov. 19, 2024).
[3] Bharatiya Nyaya Sanhita § 294 (2023).
[4] Bharatiya Nyaya Sanhita § 356 (2023).
[5] Bharatiya Nyaya Sanhita § 78 (2023)..
[6] Online Doxxing-Cyber Aware Digital Naagrik, ISEA, https://awareness.isea.app/concept/online-doxxing/what-law-says-against-such-offences#:~:text=In%20India%2C%20there%20is%20no,stalking%20(Section%20354D%20IPC) (last visited Nov. 19, 2024).
[7] India Const. art. 21.
[8] Doxxing-Police, ISEA, https://infosecawareness.in/concept/police/doxxing (last visited Nov. 19, 2024).
[9] Batuhan Kukul, Personal Data and Personal Safety: Re-examining the Limits of Public Data in the Context of Doxxing, 13 Int'l Data Privacy L. 182, 182–93 (2023).
[10] Paul Snyder et al., Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxxing, in Proceedings of the 2017 Internet Measurement Conference 432, 432–44 (2017).
[11] Les Hutchinson, Wielding Power and Doxxing Data, in The Routledge Handbook of Digital Writing and Rhetoric 323, 323-35 (Jonathan Alexander & Jacqueline Rhodes eds., 2018).
[12] India Const. art. 21
[13] This Mumbai Woman Took a Stand Against 'Brothel' Remark on Her Dance Video, Here's What Happened Next, Econ. Times (Feb. 19, 2024, 10:12 AM), https://economictimes.indiatimes.com/magazines/panache/this-mumbai-woman-took-a-stand-against-brothel-remark-on-her-dance-video-heres-what-happened-next/articleshow/107808659.cms.
[14] Vanya Verma, Legal analysis of doxxing, ipleaders (Jul. 1, 2021), https://blog.ipleaders.in/legal-analysis-doxxing/.
[15] Information Technology Act, 2000 § 43.
[16] Information Technology Act, 2000 § 66E.
[17] Information Technology Act, 2000 § 72A.
[18] Bharatiya Nyaya Sanhita § 77.
[19] Bharatiya Nyaya Sanhita § 356.
[20] Bharatiya Nyaya Sanhita § 78.
[21] Lalit Kalra, Decoding the Digital Personal Data Protection Act, 2023, EY (Aug. 23, 2023), https://www.ey.com/en_in/insights/cybersecurity/decoding-the-digital-personal-data-protection-act-2023#:~:text=The%20Digital%20Personal%20Data,collected%20offline%20and%20later%20digitized (last visited Nov. 19, 2024).
[22] Vatsal Gaur & Krishnan Sreekumar, Adawn of a New Era for Data Protection in India: An In-Depth Analysis of the Digital Personal Data Protection Act, 2023, Legal 500 (Aug. 15, 2023), https://www.legal500.com/developments/thought-leadership/a-dawn-of-a-new-era-for-data-protection-in-india-an-in-depth-analysis-of-the-digital-personal-data-protection-act-2023/ (last visited Nov. 20, 2024).
[23] AZB & Partners, Digital Personal Data Protection Act, 2023- Key Highlights, Mondaq (Sep. 1, 2023), https://www.mondaq.com/india/data-protection/1360992/digital-personal-data-protection-act-2023-key-highlights (last visited Nov. 20, 2024).
[24] Shreya Singhal v. Union of India, AIR 2015 SC 1523.
[25] Shibani Barik v. State of Odisha Opp. Party, AIRONLINE 2020 Ori 173.
[26] Swami Ramdev v. Juggernaut Books Pvt. Ltd. & Ors., AIRONLINE 2018 Del 2375.
[27] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., AIR 2017 SC 4161.
[28] Naik Naik & Co., Understanding Doxxing & Its Impact, Apr. 7, 2024, accessed Nov. 19, 2024, https://naiknaik.com/2024/04/07/understanding-doxxing-its-impact/.
[29] Richard Winton, Scarlett Johansson 'Humiliated, Embarrassed' by Celebrity Hacker, Los Angeles Times, Dec. 17, 2012, accessed Dec. 19, 2024, http://latimesblogs.latimes.com/lanow/2012/12/celebrity-hacker.html.
[30] Interstate Doxxing Prevention Act, H.R. 6478, 114th Cong. (2016), https://www.congress.gov/bill/114th-congress/house-bill/6478#:~:text=This%20bill%20amends%20the%20federal,and%20as%20a%20result%2C%20place (last visited Nov. 19, 2024).
[31] Data Protection Act 2018, GOV.UK, https://www.gov.uk/data-protection#:~:text=The%20Data%20Protection%20Act%202018,Data%20Protection%20Regulation%20(GDPR).&text=They%20must%20make%20sure%20the,used%20fairly%2C%20lawfully%20and%20transparently (last visited Nov. 19, 2024).
[32] Malicious Communications Act 1988, c. 27, § 1 (UK), https://www.legislation.gov.uk/ukpga/1988/27/section/1 (last visited Nov. 19, 2024).

[33] Communications Act 2003, c. 21, § 127 (UK), https://www.legislation.gov.uk/ukpga/2003/21/section/127 (last visited Nov. 19, 2024).
[34] Computer Misuse Act 1990, c. 18, §§ 1–4 (UK), https://www.legislation.gov.uk/ukpga/1990/18/contents (last visited Nov. 19, 2024).
[35] Doxxing—What is it?, SafeguardingHub, https://safeguardinghub.co.uk/doxxing-what-is-it/ (last visited Nov. 19, 2024).
[36] Protection from Harassment Act, 1997, https://sso.agc.gov.sg/Act/PHA2014?ProvIds=pr3- (last visited Nov. 19, 2024). –
[37] How doxxing and hate speech laws are changing in Australia, SBS News (Sept. 12, 2024), https://www.sbs.com.au/news/article/how-doxxing-and-hate-speech-laws-are-changing-in-australia/ofzfcji75 (last visited Nov. 19, 2024).
[38] Michelle Wan, An Overview of the New Anti-Doxxing Regime, Deacons (May 22, 2023), https://www.deacons.com/2023/05/22/an-overview-of-the-new-anti-doxxing-regime/ (last visited Nov. 19, 2024).
[39] Netherlands: Doxxing Criminalised, Library of Congress, https://www.loc.gov/item/global-legal-monitor/2023-08-01/netherlands-doxxing-criminalized/ (last visited Nov. 19, 2024)

