SECTION 78 BNS: CYBERSTALKING, GENDER AND DIGITAL EVIDENCE IN CONTEMPORARY INDIA

Rucha Kankal, Pravin Gandhi College of Law

Introduction

Cyberstalking and online harassment have emerged as pressing challenges under India's new criminal laws. The **Bharatiya Nyaya Sanhita, 2023 (BNS),** which overhauls the country's penal code, expressly criminalises stalking and intimidation in Sections 78 and 351. Section 78 of BNS defines *"stalking"* by focusing on a man repeatedly contacting or electronically monitoring a woman, even if she's made it clear she isn't interested [1]. Section 351(4) similarly punishes anonymous or masked threats under *"criminal intimidation"*[2]. Both these provisions carry imprisonment (first offence up to 3 years, repeat up to 5 years) and fines, aligning with the replaced IPC definitions. The Information Technology Act, 2000, supplements these with offences like identity theft (Sec 66C)[3], online impersonation (Sec 66D) [4]and transmission of obscene (Sec 67) [5]or explicit sexual material (Sec 67A) electronically[6]. So, with the BNS and IT Act together, India has built a legal structure meant to tackle digital stalking and harassment.

This paper studies those provisions, examines evidence rules (Bharatiya Sakshya Adhiniyam, 2023) and procedures (Bharatiya Nagarik Suraksha Sanhita, 2023), work in practice, looks at key court decisions, and considers gender and child rights perspectives. It also compares the new system to the old IPC regime. At the end, it looks at the practical hurdles like anonymity, cross-border jurisdiction, and whether tech platforms cooperate and offer concrete legal and policy fixes.

Cyberstalking and Harassment in the BNS, 2023

Section 78 (Stalking). Under the BNS, stalking is defined narrowly in gendered terms: "Any man" who (i) follows a woman and repeatedly contacts her despite clear disinterest, or (ii)

[1] BNS,2023 ,S.No. 78 , Acts of Parliament, 2023 (India).
[2] Section 351(4) - The Bharatiya Nyaya Sanhita, 2023
[3] Section 66C in The Information Technology Act, 2000
[4] Section 66D in The Information Technology Act, 2000
[5] Section 67 in The Information Technology Act, 2000
[6] Section 67A in The Information Technology Act, 2000

monitors a woman's internet, email or electronic communications, commits stalking[7]. This follows IPC section 354D but puts emphasis on digital monitoring. The statute sets the punishment for first-time offenders of up to three years' imprisonment (and fine), and up to five years on conviction for repeat offences. The provisions are accompanied by justifications (for example, police action is excluded if done to detect crime).In effect, Section 78 directly targets men who harass women, online or off, and tries to close legal gaps that once let digital stalkers slip through.

Section 351(4) (Anonymous Threats). Section 351 of the BNS tackles criminal intimidation, and its fourth subsection makes things tougher for people who issue threats anonymously. In plain terms, if someone threatens another person but hides their identity, maybe through an anonymous message or a spoofed account, they're looking at up to two extra years in prison on top of the usual sentence for intimidation. This isn't new; it's more or less a direct carryover from the old IPC Section 507, which also targeted anonymous threats. So, when it comes to online harassment, those hidden, untraceable messages or fake profiles, BNS doesn't leave any grey area. Section 351(1) already defines intimidation pretty broadly, covering threats to someone's person, reputation, and so on. If you can show that the person was meant to intimidate, even cyber threats fall under this. Section 351(4) specifically goes after the all-too-common trick of using untraceable accounts to threaten people online.

Put together, these rules cover a lot of what we call "cyber harassment" the following, contacting, and intimidation that happens both online and off. But there's a catch. The law's language is still gendered, focused on threats, and mostly pictures men threatening women. Section 78 and Section 351(4) both talk about male-on-female scenarios. This leaves a real gap—what about men or non-female victims? And the law seems more worried about harm to reputation or mental state than about physical threats.

Related IT Act Provisions

The BNS makes stalking and threats crimes, while the Information Technology Act, 2000, provides complementary cyber offences. Include Key Sections

- **Section 66C (Identity Theft):** An individual who uses someone else's electronic

[7] Bharatiya Nyaya Sanhita, 2023, Section 78

signature, password, or unique identification feature in a fraudulent or dishonest manner is liable for up to three years of imprisonment and a fine of up to ₹1 lakh. This covers online impersonation and identity fraud. For instance, if someone masquerades as the victim and creates their social media profile or sends a message, that too would allow charging them under S.66C.[8]

- **Section 66D (Definition of Cheating Act by Personation)**: Anyone who impersonates another person by means of communication using a computer resource would be penalised under this with a jail term of three years and a ₹1 lakh fine. It covers online impersonation schemes where a person has posed as another person for extortion or deception. When false online identities or false emails are used, Section 66D may come into operation in the harassment context.[9]

- **Section 67(prohibits obscene electronic content)**: Publishing or broadcasting any material that is lewd or appeals to the prurient interest with a computer or any other electronic means is punishable up to 3 years' imprisonment (first offence) or 5 years (repeat), with hefty fines. This involves posting of general obscenity or pornography. To illustrate, the distribution of revenge porn (non-explicit but defamatory images) has been prosecuted under S.67 (as in Suhas Katti v. Tamil Nadu).

- **S.67A (Sexually Explicit Material)l**: This clause deals with online sexually explicit content. First-time offenders could face 5 years in jail and a fine of up to ₹10 lakh; repeat offenders could face up to 7 years' jail and ₹10 lakh. The site is dedicated to hardcore pornographic content. While S.67A is (mostly) about consensual porn, courts sometimes try to apply it (or the missing S.67B) to "revenge porn."[10]

The provisions of the IT Act intersect with the BNS stalking law. In the Kalandi Charan Lenka v. State of Odisha case[11], For instance, the accused was charged under different sections of the Indian Penal Code. 354A and 354D, and sections 66C, 66D, 67 and 67A of the IT Act for sending defamatory messages and for creating a fake Facebook account containing nude photos of the victim.

[8] Information Technology Act 2000, s 66C.
[9] Information Technology Act 2000, s 66D
[10] Information Technology Act 2000, s 67A.
[11] *Kalandi Charan Lenka v State of Odisha* 2017 SCC OnLine Ori 418

Provisions of section 66C/D (for fake identity) and section 67A (for pornographic images) shows IT offences bolster laws on BNS harassment. The Supreme Court in Shreya Singhal v. UOI (2015)[12] observed that Section 66A of the IT Act (offensive messages) is violative of free speech. This part of the act was often used to target online harassment. Consequently, the wide provisions punishing "annoyance" cannot be invoked now, limiting prosecutorial tools.

Evidence and Procedure under BSA and BNSS

New evidentiary and procedural rules guide cyber harassment cases. The **Bharatiya Sakshya Adhiniyam, 2023 (BSA)** (India's Evidence Act) and the **Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)** (CrPC replacement) contain several relevant sections.[13]

- **BSA S.57 (Primary Evidence).** This defines "primary evidence" as the document itself produced for inspection[14]. Crucially, it includes explanations extending to electronic documents. If an electronic record is printed, stored or transmitted in multiple files, "each such file" is treated as primary evidence. Thus, server logs, chat logs, emails or multiple backups are each primary evidence of content. This clarification accommodates the digital nature of cybercrime evidence: a forensic copy of a chat transcript or email may be admitted as the original document itself.[15]

- **BSA S.63 (Computer Output as Document).** Any information contained in a computer-generated record, when printed or stored, is deemed a *"document"* if authenticated[16]. In effect, computer outputs – such as forensic printouts, CD/DVD copies of chats, or email archives – are admissible as documentary evidence, subject to certificate requirements. The scheme follows the former §65B (IEA) but is integrated into the law. For example, a certified printout of an email threatening a victim would count as secondary evidence of its contents under S.63 if proper conditions are met. These rules ease the prosecution of cyber offences by allowing digitally stored evidence

[12] *Shreya Singhal v Union of India* (2015) 5 SCC 1.
[13] Bharatiya Sakshya Adhiniyam, 2023; Bharatiya Nagarik Suraksha Sanhita, 2023 (Acts 2023 replacing the Indian Evidence Act, 1872 and Code of Criminal Procedure, 1973)
[14] Bharatiya Sakshya Adhiniyam, 2023, s. 57
[15] Law Commission of India, *Report No. 185 on Review of the Indian Evidence Act* (2003)
[16] Bharatiya Sakshya Adhiniyam, 2023, s. 63(1)–(3)

to be admitted under normal documentary standards, provided the mandatory machine certification (now in §63(2)–(3)) is supplied.

- **BNSS S.105 (Audio-Video Search Record).** Section 105 mandates that during any search or seizure (under BNSS Chapter) – including search of a digital device – the entire process be recorded via audio-video (e.g. by mobile phone) and promptly forwarded to a magistrate[17]. This is modelled on recent CrPC amendments[18]. In cyber harassment cases, where police seize computers, phones or storage, §105 ensures transparency: the list of seized items and search procedure must be filmed. This guards against tampering and establishes a credible chain of custody for digital evidence. It also covers any search under telegraph or criminal law (Sec.185 references in the text).

Together, BSA S.57 and S.63 broaden the admissibility of electronic data (email transcripts, IP logs, metadata) in harassment trials, while BNSS S.105 strengthens procedural safeguards in gathering such evidence.[19] Prosecutors can thus rely on certified e-records and video-recorded raids, bolstered by witness testimony.

Key Judicial Precedents

Several Indian cases illustrate cyberstalking and harassment under the old and new laws:

- **Kalandi Charan Lenka v. State of Odisha (2017, Ori HC).** The Orissa High Court looked at a case where a woman faced relentless harassment via emails, obscene letters, pamphlets, plus a fake Facebook page set up to defame her. The accused bombarded her with vulgar messages (charged under IPC Sections 294, 354A, and 354D) and even created doctored naked images using a spoofed account (IT Act Sections 66C, 66D, 67, 67A). The case was mainly about bail, but the court still took a firm line: the pattern of anonymous messages added up to stalking and intimidation. The High Court backed the charges of identity crimes, explicit content, stalking, and insulting gestures or words. What stands out is how cyberstalking usually mixes online and offline behaviour. And even though this case used the IPC and IT Act, the facts fit almost

[17] **.** Bharatiya Nagarik Suraksha Sanhita, 2023, s. 105
[18] Code of Criminal Procedure (Amendment) Act, 2008
[19] Aparna Chandra & Mrinal Satish, *Criminal Law and the Constitution* (Oxford University Press 2020) 312–318

perfectly under the current BNS Sections 78 and 351(4).

- **Animesh Boxi v. State of West Bengal (2018, JM).** Known as India's first "revenge porn" case, Animesh Boxi was convicted for uploading intimate photos and videos of his ex-girlfriend on pornographic websites. The JM (Tamluk) sentenced him to 5 years' rigorous imprisonment (₹9,000 fine), applying multiple IPC and IT Act provisions (including §§354D, 509 IPC for stalking/insult and §§66C/D IT Act for identity misuse). The court emphasized that no physical violence was needed: "injury to reputation falls within the ambit of 'injury' as laid down in Section 44 of the IPC," and his online stalking with intimate images amounted to outraging the victim's modesty. This landmark case signals that cyber harassment targeting female dignity is severely penalised. Under BNS, Boxi's acts would be prosecuted as stalking (§78) and intimidation (§351) in addition to IT Act offences.

- **Suhas Katti v. State of Tamil Nadu (2004, Met. Mag.).** A seminal case in cyber harassment law, Suhas Katti was the first person convicted under the IT Act[10]. He had sent obscene, defamatory Yahoo messages and emails to a divorced woman, set up a fake account in her name to forward her mail, and caused strangers to call her phone. The court accepted electronic evidence under the (old) Section 65B, and held Suhas guilty of IPC §§469 (forgery), 509 (insulting modesty) and IT Act §67[10]. He was sentenced to two years' rigorous imprisonment (RI) for forgery, one year SI under §509, and two years RI under §67 (all to run concurrently)[10]. The conviction demonstrated early judicial willingness to treat online harassment seriously. Notably, §67 IT Act (obscene transmission) was used instead of the then-pending §66A. Under current law, his conduct (creating fake emails, harassing calls) would fall under BNS stalking (§78) and intimidation (§351), as well as §§66C/D (impersonation). • Notably, the then-pending §66A was replaced with the §67 IT Act (obscene broadcast). His actions (making fictitious emails and pestering calls) would be considered BNS stalking (§78), intimidation (§351), and impersonation (§§66C/D) under the present legislation.

- **Shreya Singhal v. Union of India (2015, SC).** Though not a "harassment" case per se, Shreya Singhal is pivotal. The Supreme Court struck down IT Act §66A (offensive electronic messages) as violative of free speech[13]. This decision invalidated a broad tool that had been used by some courts against abusive online speech (e.g. emails or

posts aimed at "annoyance" or "insult"). Its implications for cyber harassment law are mixed: on one hand, it protects legitimate speech, but on the other, it removes a catch-all provision. Now, prosecutions must rely on the narrower stalking, harassment and intimidation provisions (BNS §78,351 etc) or defamation laws, rather than the open-ended "grossly offensive" standard of §66A[13].

The fact that unsolicited electronic communications that cause fear or harm to one's reputation might be illegal is further supported by other examples (such as S. Natarajan v. Govt. of Tamil Nadu on threats via SMS or other high court decisions on IPC 354D). The aforementioned examples demonstrate how the courts handled digital harassment before to BNS; comparable circumstances under BNS are likely to result in conviction, albeit under the new sections.

Feminist and Child Rights Perspectives

Because these offences are highly targeted, there is a need for an age- and gender-based analysis. The feminist push for safeguarding women from male stalking is evident in Section 78, which gives explicit protection [20]. On the one hand, this acknowledges that harassment that takes place in the street and online is largely attributed to women. The victims of cyberstalking experience serious psychological harm, fear, and ostracism. The central aspect of the legislation (the protection of "modesty" and mental peace) is praiseworthy because it reaffirms female dignity and safety. When put into practice, courts are aware of the compounded effect of online abuse on women. In Animesh Boxi' case, for instance, the court emphasised that "injury" to the female victim's reputation through intimate images is an injury that deserves strict punishment[21].

On the flip side, BNS's gender exclusivity raises dilemmas. According to section 78, men are the only ones who can end up in a stalking case. Critics say cyberstalkers have no gender, so a gender-neutral law (or one that protects all genders) may be more apt. The law focuses on the notions of honour that derive from traditional views of modesty and sexual reputation and does not reflect other forms of abuse, such as harassment based on religion, caste or on male victims' personal space. A progressive lens would include all genders in the ambit of protection, and cyber harassment affecting men and transgender individuals should also be equally punishable. In addition, the law sensibly revolves around notions of "modesty" as well as sexual reputation,

[20] Bharatiya Nyaya Sanhita, 2023, s. 78
[21] *State of West Bengal v. Animesh Boxi*, Criminal Case No. 06 of 2018

which are traditional notions of honour. This may miss out on other types of abuse. This includes harassment based on one's religion, caste or on the personal space of male victims. An inclusive lens would mean applying the protection to all genders and treating cyber harassment against men and the transgender community as equally punishable.

A perspective based on child rights adds more layers. Minors including both children and teenagers have special vulnerability online either because of cyber bullying, grooming or exposure to sexual content. [22]While BNS S.78 relates to women, "stalking" of minors can also happen (e.g. constant messaging for surveillance of a girl). Even if the BNS does not specifically address kid online harassment, other laws apply. Under POCSO, it is illegal to use digital child pornography (Section 3) or sexually harass minors online.[23]

Prior to the introduction of the BNS, child porn was explicitly dealt with by section 67B of the IT Act. However, this provision has now been removed and has been covered under more elaborate laws like POCSO. A man who stalks a young girl online will face more than just BNS stalking. He will also be booked under the POCSO laws for posting her photos online.

According to feminists and child advocates, internet abuse is gendered and impactful. Research indicates that women's harassment that silences them in online spaces occurs as a result of misogynistic norms in digital spaces.[24] It can inflict psychological harm on children [25] . Both perspectives call for effective enforcement and support for victims. The recommended solutions include help lines, gender-sensitive cybercrime units, and instruction on digital consent. Also, it's called for legal reforms such as widening the stalking law to protect both sexes or fast-tracking courts for cybercrime against children.

IPC S.354D: Stalking.

BNS Section 78 is almost identical to IPC section 354D, which was introduced into the statute in 2013. In the same way, stalking by a man is defined at Section 354D(1) as applying to a man who follows a woman and who contacts or attempts to contact her repeatedly despite a clear indication of disinterest by or on behalf of the woman or who monitors a woman's internet

[22] E. Livingstone et al., *EU Kids Online 2020: Survey Results from 19 Countries* (London School of Economics, 2020)
[23] Protection of Children from Sexual Offences Act, 2012, ss. 3 & 11
[24] UN Women, *Online and ICT-facilitated violence against women and girls* (2020)
[25] UNICEF, *Children in a Digital World: State of the World's Children Report* (2017)

activity and other such acts.[26]The structure of the punishment was the same (punishment up to 3 years and fine; 5 years for repeat). In essence, there is nothing new in section 78; it is just differently named. It still utilises the man-woman formulation. 354D is still faced with past issues like the gender binary, and that 'repeated' acts are required. Some critics say “repeatedly” might be too strict (because one act of cyberharassment might be ongoing by nature), BNS keep this term. There may be no corresponding IPC §354D(3), which permitted appropriate behavior. Nonetheless, BNS explains that unreasonable behaviour, such as police monitoring, is not stalking.

In short, BNS keeps the IPC's anti-stalking rules with only a few changes. The historical position persists: cyberstalking constitutes a criminal offense, particularly when the victim is female. There is a nod to feminist reasoning, but most of the criticisms of IPC section 354D (narrow focus) still stand

Enforcement Challenges

Despite these laws, cyberstalking cases present practical hurdles:

- **Anonymity and Traceability:** Pseudonyms, VPNs, burner phones, or phony profiles are common ways for online harassers to conceal. [27]It takes technical expertise and platform cooperation to link anonymous messages or social media profiles to a real person. [28]Although anonymous threats are punishable under Section 351(4), it is nevertheless challenging to identify the perpetrator. Even if the law permits a longer punishment, it can be difficult to determine "who" the real offender is. Since they may be stored abroad or swiftly deleted, law enforcement organizations frequently have difficulty obtaining timely data (such as IP logs) from service providers[29]. Although audio-video documentation of device seizures is required under BNSS S.105, it can be difficult to prove that a specific suspect used the device at the time, particularly if it was locked or encrypted.

- **Jurisdictional Issues.** Cyberbullying can occur across national and state boundaries. Questions of investigative jurisdiction, extradition, and applicable law come up when a

[26] Indian Penal Code, 1860, s. 354D (inserted by Criminal Law (Amendment) Act, 2013)
[27] K Jaishankar, *Cyber Criminology: Exploring Internet Crimes and Criminal Behaviour* (CRC Press 2011).
[28] Nir Kshetri, *Cybercrime and Cybersecurity in India* (Springer 2013
[29] Susan W Brenner, *Cybercrime: Criminal Threats from Cyberspace* (Praeger 2010).

harasser from another state or nation attacks a victim in India. For instance, a foreign Instagram user who posts disparaging content about an Indian user may be in conflict with both Indian law and international privacy rights. Although the IT Act has certain measures (such as blocking under Section 69A and intergovernmental cooperation under Section 78), enforcement is still developing. [30]Quick action is hampered in several sectors (such as revenge porn sites) by the absence of consistent international cybercrime treaties[31]. The resources and priorities of the cyber cells in various Indian states may differ, resulting in uneven responses.[32]

- **Platform Cooperation and Safe Harbors.** Important evidence can be found in messaging apps and social media (messages, IP logs). Intermediaries have little accountability under the IT Act as long as they follow the proper procedures, although law enforcement frequently needs their assistance[33]. In reality, social media sites like Facebook and WhatsApp might object to disclosing user information without following the proper procedures[34]. Encryption (particularly end-to-end, like on WhatsApp) prevents even the firm from reading conversations, even when subpoenaed[35]. Police can seize devices under Section 105 BNSS (recording searches) and BSA Section 63/57, however content on cloud or third-party servers may be difficult to obtain. Furthermore, the emphasis on "electronic records" in the statute assumes cooperation, which is not always the case.

- **Proving Mens Rea and Effects.** Proof of intent to harass or alarm is required by courts. Although suspects frequently deny knowing, purpose in internet crimes can be deduced from the context and content of messages. Judges may find it difficult to measure the mental anguish of victims. A plethora of statements and actions, for example, was deemed adequate in Kalandi Charan Lenka to suggest intent to insult modesty. [36]However, proof may be circumstantial in the absence of a clear IP log or a direct confession. [37]The victim's testimony and digital records are sometimes the only

[30] Bharatiya Nyaya Sanhita 2023, s 351(4)
[31] Council of Europe, *Convention on Cybercrime* (Budapest, 2001)
[32] Ministry of Home Affairs, *Cyber Crime Prevention against Women and Children (CCPWC) Scheme* (India)
[33] Information Technology Act 2000, s 79.
[34] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021, rr 3, 4
[35] Justice KS Puttaswamy (Retd) v Union of India (2017) 10 SCC 1.
[36] Kalandi Charan Lenka v State of Odisha 2017 SCC OnLine Ori 418.
[37] Anvar PV v PK Basheer (2014) 10 SCC 473.

witnesses left by cyber harassment; courts must then carefully assess the veracity of screenshots or recordings. [38]Although the BSA's regulations help, there are still gaps.

In sum, enforcing the new laws requires sophisticated cyber-investigation infrastructure and legal cooperation. The letter of law is strong, but practical barriers – anonymous technologies, cross-border networks and platform policies – often impede prosecution. [39]Addressing these challenges requires not only legal tools but also capacity building.[40]

Recommendations

To make the cyber harassment framework actually work, we need to take some concrete legal and policy steps:

Gender-Neutral Provisions: Amend Section 78 and related stalking laws so they protect everyone, regardless of gender, from stalking and digital harassment. Accepted that women face the brunt of these attacks, but men and members of the LGBTQ+ community are targeted too. A gender-neutral clause, following UNHRC guidance, gives broader protection and avoids running into constitutional problems.

Victim Protection and Support: Establish specialised cyber cells or fast-track courts for cases of harassment, particularly those involving women and children. Victims require access to counselling and anonymity. Take POCSO's kid-friendly protocols and modify them for use in cyber trials when minors are involved.

More Robust Evidence Guidelines: Provide a clause requiring intermediaries to retain and promptly provide data, such as electronic discovery orders. Although the BSA already permits the admission of electronic records, prosecution requires that ISPs have shorter data retention periods and be required to disclose information when necessary. Clear guidelines regarding the admissibility of novel types of evidence, like deepfake detection reports, should be provided to courts.

International Cooperation: To enable authorities to quickly track down accounts abroad, we should begin negotiating mutual legal assistance treaties centered on cyber harassment as a

[38] Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1
[39] UNODC, *Comprehensive Study on Cybercrime* (2013
[40] Law Commission of India, Report No 267 (Data Protection and Privacy).

country. Extradition agreements are necessary for serious cybercrimes in India. It's also time to reexamine multilateral frameworks that facilitate the exchange of evidence, such as the Budapest Convention.

Platform Accountability: Demand that large social media companies establish transparent, easily accessible procedures for managing complaints of harassment without infringing on privacy. Encourage them, as Germany and the UK have done with their "revenge porn" laws, to establish gender-sensitive review boards and take prompt action to remove non-consensual intimate images. Examine a legal "duty of care" that would hold platforms accountable for hosting harassing content with knowledge and failing to take appropriate action.

Digital literacy and public awareness: Start initiatives to inform people of their rights online and available remedies. Encourage people to report cyberstalking in addition to discussing how serious it is. Put a special emphasis on empowering women and children, maybe by offering courses at schools and universities on legal options and online safety. Simple, uncomplicated instructions on how to file complaints under the BNS or IT Act regulations should be available on the central portal under the IT Act.

Research and Legislative Review: Establish routine reviews of cyber harassment laws as society and technology evolve, perhaps through the Law Commission. To help shape wise policy, support scholarly investigations into cyber abuse trends. For example, feminist legal scholarship can identify blind spots in enforcement.

A strong mechanism for the successful deterrence of online harassment is provided by the thoughtful application of these measures. Even though the Information Technology Act and the Bharatiya Nyaya Sanhita (BNS) create a strong legal framework, legislation alone is still a "paper tiger." A synergistic partnership between a technologically savvy judiciary, a specialised law enforcement apparatus, and extensive digital literacy programs is necessary for the realisation of digital safety. India can fulfil its constitutional mandate to protect its citizens' dignity, especially that of women and children, from the widespread evolution of abuse enabled by cyberspace by bridging the gap between legislative intent and institutional execution.