

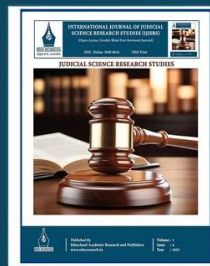


INTERNATIONAL JOURNAL OF JUDICIAL SCIENCE RESEARCH STUDIES (IJJSRS)

(Open Access, Double-Blind Peer Reviewed Journal)

ISSN Online: 3049-0618

ISSN Print: 3108-2785



Legal Frameworks Protecting Domestic Violence Survivors Digitally

Adwaidh Jaimon

4th year Student, BBA LL.B. (Hons), Cooperative School of Law, Thodupuzha, India

Article information

Received: 4th June 2026

Received in revised form: 2nd July 2026

Accepted: 10th August 2026

Available online: 21st August 2026

Volume: 3

Issue: 3

DOI: <https://doi.org/10.63090/IJJSRS/3049.0618.0047>

Abstract

The digital age has fundamentally transformed the landscape of domestic violence, creating new avenues for abuse while simultaneously challenging traditional legal frameworks designed to protect survivors. This paper examines the evolution of legal protections for domestic violence survivors confronting technology-facilitated abuse, analyzing recent legislative developments including the Violence Against Women Act Reauthorization of 2022, the federal Take It Down Act of 2025, and state-level coercive control legislation. Through critical analysis of international conventions, federal statutes, and emerging case law, this study reveals persistent gaps in legal frameworks despite progressive reforms. The paper argues that effective protection requires interdisciplinary approaches integrating criminal law, civil remedies, platform accountability, and survivor-centered policies. By examining the intersection of technology, law, and gendered violence, this research contributes to ongoing debates about digital safety, privacy rights, and the modernization of domestic violence law to address 21st-century threats.

Keywords:- Domestic violence, cyberstalking, coercive control, survivors, Take It Down Act, digital abuse

I. INTRODUCTION

Domestic violence, historically understood as physical and sexual abuse within intimate relationships, has undergone a profound transformation in the digital age. Technology-facilitated domestic abuse (TFDA) now encompasses cyberstalking, non-consensual intimate image distribution, GPS tracking, account hacking, and digital coercive control--tactics that extend an abuser's reach beyond physical proximity (Harris & Woodlock, 2019). The ubiquity of smartphones, social media platforms, and Internet of Things devices has created unprecedented opportunities for surveillance, harassment, and manipulation, fundamentally altering the dynamics of intimate partner violence.

Legal frameworks designed to protect domestic violence survivors have struggled to keep pace with technological evolution. Traditional restraining orders and assault statutes, crafted in an era of localized physical violence, prove inadequate when confronting digital abuse that transcends geographic boundaries and operates continuously through networked devices. As intimate partner violence affects over 10 million individuals annually in the United States alone (Centers for Disease Control and Prevention, 2024), the imperative to modernize legal protections has never been more urgent.

This paper critically examines the legal frameworks emerging to address digital-age domestic violence. It analyzes international conventions, federal legislation, and state-level reforms while interrogating their efficacy in protecting survivors from technology-facilitated abuse. Through this analysis, the paper illuminates both the progress achieved and the persistent gaps requiring further legislative attention.

II. THEORETICAL FRAMEWORK

Understanding legal responses to digital domestic violence requires engagement with multiple theoretical frameworks. The *power and control model*, developed by domestic violence advocates and articulated through the Duluth Model's Power and Control Wheel, provides foundational understanding of how abusers maintain dominance through systematic tactics including intimidation, isolation, economic abuse, and emotional manipulation (Pence & Paymar, 1993). Technology amplifies

each spoke of this wheel: digital surveillance enables constant monitoring, social media facilitates public humiliation, financial apps provide tools for economic control, and smart home devices create new mechanisms for intimidation.

Feminist legal theory illuminates how digital domestic violence perpetuates gendered power structures. Though anyone can experience technology-facilitated abuse, women disproportionately suffer from non-consensual intimate image distribution, cyberstalking, and digital sexual harassment (Powell & Henry, 2019). Legal frameworks failing to recognize technology-facilitated abuse as serious violence effectively perpetuate patriarchal systems that minimize women's experiences and maintain male dominance through fear and control.

The concept of *coercive control* provides crucial theoretical grounding. Developed by Evan Stark, coercive control describes domestic violence as a pattern of strategic behaviors designed to dominate another person through intimidation, isolation, and deprivation rather than discrete physical assaults (Stark, 2007). Digital technologies enhance coercive control by enabling continuous surveillance, instantaneous communication of threats, and inescapable monitoring that follows survivors into every aspect of their lives. This theoretical framework has proven particularly influential in recent legislative reforms recognizing non-physical abuse as actionable domestic violence.

III. THE EVOLUTION OF LEGAL FRAMEWORKS: FROM PHYSICAL VIOLENCE TO DIGITAL ABUSE

Modern domestic violence law emerged from feminist activism in the 1970s that challenged law enforcement's reluctance to intervene in family matters and courts' failure to protect battered women. The Violence Against Women Act of 1994 marked a watershed moment, establishing federal leadership in addressing gender-based violence and authorizing over \$1.6 billion for investigation, prosecution, and victim services (Violence Against Women Act, 1994). VAWA's original focus centered on physical violence, sexual assault, and stalking understood primarily through pre-digital paradigms.

The 2000 reauthorization began addressing technology's role by including dating violence and stalking provisions. The 2005 reauthorization represented the first explicit recognition of cyberstalking, expanding federal stalking definitions to encompass electronic communications and surveillance (Violence Against Women and Department of Justice Reauthorization Act, 2005). The 2013 reauthorization strengthened tribal jurisdiction and explicitly addressed cyberstalking using any interactive computer service or electronic communication service (Violence Against Women Reauthorization Act, 2013).

Most significantly, the 2022 VAWA Reauthorization Act introduced comprehensive definitions of technological abuse as acts or patterns of behavior intended to harm, threaten, intimidate, control, stalk, harass, impersonate, exploit, extort, or monitor another person using technology (Violence Against Women Act Reauthorization Act, 2022). This definitional expansion acknowledged that technology-facilitated abuse constitutes a distinct form of violence requiring specialized legal responses. The 2022 reauthorization also authorized grant programs specifically targeting cybercrimes against individuals and established a National Resource Center on Cybercrimes to provide training for law enforcement and judicial personnel.

IV. TECHNOLOGY-FACILITATED DOMESTIC ABUSE: MANIFESTATIONS AND MECHANISMS

Technology-facilitated domestic abuse encompasses diverse tactics that exploit digital infrastructure to perpetuate control and harm. *Surveillance and monitoring* include GPS tracking through phone applications, spyware installation, keylogging software, unauthorized access to email and social media accounts, and exploitation of smart home devices to monitor survivors' movements and communications (Freed et al., 2018). Such pervasive surveillance creates a psychological state of constant monitoring that survivors describe as inescapable, extending abusers' reach into spaces traditionally considered safe.

Image-based sexual abuse, commonly termed revenge porn, involves non-consensual distribution of intimate images to humiliate, intimidate, or coerce survivors. With the advent of artificial intelligence, deepfake pornography--digitally fabricated explicit images appearing to depict real individuals--has emerged as a particularly pernicious form of technological abuse (McGlynn et al., 2017). The threat of image distribution functions as a powerful tool for coercion, forcing survivors to comply with abusers' demands under threat of public humiliation and professional destruction.

Cyberstalking encompasses repeated unwanted communications through email, text messages, social media, and online forums that cause substantial emotional distress or fear. The persistent, boundary-crossing nature of digital communications means survivors cannot escape their abusers by changing physical locations; harassment follows them into every digital space they inhabit. Additionally, *identity theft and impersonation* enable abusers to create fake accounts in survivors' names, post defamatory content, damage professional reputations, and manipulate survivors' social networks (Douglas et al., 2019).

Research indicates that technology-facilitated abuse rarely occurs in isolation but typically accompanies or escalates into physical violence. Survivors experiencing digital coercive control report higher rates of physical assault, sexual violence, and fear for their safety (Dragiewicz et al., 2018). This interconnection underscores the necessity of legal frameworks that recognize technology-facilitated abuse not as a separate category but as integral to contemporary domestic violence patterns.

V. RECENT LEGISLATIVE DEVELOPMENTS: FEDERAL AND STATE RESPONSES

The landscape of legal protections for survivors of digital domestic violence has transformed dramatically between 2022 and 2025. At the federal level, the Take It Down Act, signed into law in May 2025, represents the first comprehensive federal criminalization of non-consensual intimate image distribution (Take It Down Act, 2025). The legislation establishes criminal penalties for knowingly publishing or threatening to share intimate images without consent, including AI-generated deepfake pornography depicting identifiable individuals. Significantly, the Act imposes differential penalties based on victim age: violators face up to two years imprisonment for adult victims and three years for minor victims.

The Take It Down Act also establishes platform accountability requirements, mandating that social media companies, hosting services, and online forums remove non-consensual intimate imagery within 48 hours of notification and implement reasonable measures preventing reposting. This provision addresses the viral nature of digital abuse, where images circulate rapidly across platforms, causing ongoing harm. However, critics note that 48-hour removal timeframes may prove insufficient given the speed of digital distribution and the psychological trauma inflicted even by brief exposure (Franks, 2023).

State-level reforms have demonstrated particular innovation in recognizing coercive control as actionable domestic violence. Massachusetts's Act to Prevent Abuse and Exploitation, enacted in June 2024, criminalized non-consensual intimate image distribution while expanding the definition of abuse under protective order statutes to include coercive control (Commonwealth of Massachusetts, 2024). The legislation defines coercive control as a pattern of behavior intended to threaten, intimidate, harass, isolate, control, coerce or compel compliance of a family or household member that causes fear or a reduced sense of physical safety or autonomy. This definition explicitly encompasses threatening to share explicit images, regulating communications and access to services, and isolating victims from support networks.

By September 2024, Massachusetts became one of the first states to operationalize coercive control provisions, enabling survivors to obtain restraining orders based solely on patterns of non-physical abuse including digital harassment and technological control (Domestic Violence Services Network, 2024). As of mid-2025, all 50 states have enacted criminal statutes addressing non-consensual intimate image distribution, representing remarkable legislative progress achieved through sustained advocacy by survivors, anti-violence organizations, and legal scholars.

VI. IMPLEMENTATION CHALLENGES AND PERSISTENT GAPS

Despite progressive legislative reforms, significant challenges impede effective protection of survivors confronting technology-facilitated abuse. *Enforcement gaps* remain pronounced. Law enforcement officers frequently lack training to recognize and investigate digital domestic violence, viewing online harassment as less serious than physical assault (Bond & Tyrrell, 2021). Police responses to image-based sexual abuse reveal limited understanding of relevant legal frameworks and insufficient confidence investigating cases or supporting survivors.

Jurisdictional complexities compound enforcement challenges. Digital abuse transcends geographic boundaries, with abusers potentially located in different states or countries from their victims. Cross-border cooperation remains inadequate, and international legal frameworks provide minimal recourse for survivors whose abusers operate from jurisdictions with weak or non-existent digital abuse legislation. Even within the United States, variations in state laws create patchwork protections dependent on survivors' locations rather than consistent federal standards.

Platform accountability presents ongoing challenges. While the Take It Down Act mandates content removal within 48 hours, enforcement mechanisms remain unclear. Questions persist regarding liability for platforms failing to comply, procedures for survivors to request removals, and verification processes preventing misuse. Section 230 of the Communications Decency Act, which shields internet platforms from liability for user-generated content, complicates efforts to hold technology companies accountable for facilitating abuse through inadequate moderation policies.

Evidence collection poses particular difficulties in technology-facilitated abuse cases. Digital evidence is easily deleted, devices may be shared or controlled by abusers, and survivors often lack technical knowledge to preserve evidence effectively. Forensic analysis requires specialized expertise and resources that many jurisdictions cannot provide. Furthermore, privacy protections--though essential--can complicate evidence gathering when abusers exploit encrypted communications and privacy-protective technologies to evade detection.

Victim-blaming narratives persist, particularly regarding image-based abuse. Legal proceedings and public discourse frequently focus on survivors' decisions to create intimate images rather than perpetrators' violations of consent and privacy. This victim-blaming approach, evident in questions about why survivors allowed images to be taken, reflects broader rape culture dismissing women's autonomy and excusing male violence. Such attitudes deter survivors from seeking legal remedies and perpetuate shame undermining recovery.

VII. IMPLICATIONS FOR LEGAL PRACTICE AND POLICY DEVELOPMENT

Addressing technology-facilitated domestic abuse requires comprehensive approaches integrating multiple legal and social interventions. First, *specialized training programs* must educate law enforcement, prosecutors, judges, and victim advocates about digital abuse manifestations, investigation techniques, and trauma-informed responses. The 2022 VAWA reauthorization authorized funding for such training, but implementation remains inconsistent across jurisdictions. Investment in continuing education ensuring criminal justice professionals understand technology-facilitated abuse as serious violence meriting robust responses is essential.

Second, *platform regulation* must expand beyond content removal mandates to address design features enabling abuse. Technology companies should implement safety-by-design principles, conducting impact assessments evaluating how platform features might facilitate abuse and developing interventions preventing misuse. Transparency requirements compelling platforms to report abuse prevalence, response times, and mitigation strategies would enhance accountability and enable data-driven policy improvements.

Third, *survivor-centered legal remedies* must prioritize victims' needs and safety. This includes expedited protective order processes addressing digital harassment, civil damages enabling survivors to sue perpetrators for economic and emotional harm, and support services providing technical assistance, mental health counseling, and legal advocacy. Massachusetts's diversion programs for youth who share explicit images represent innovative approaches balancing accountability with education, recognizing that criminal prosecution may prove counterproductive for adolescents requiring guidance rather than incarceration.

Fourth, international cooperation frameworks must develop to address cross-border digital abuse. The Council of Europe's Istanbul Convention provides a model for international domestic violence standards, but technological provisions

require strengthening and broader ratification. Bilateral agreements facilitating evidence sharing, extradition for digital abuse offenses, and coordinated platform regulation would enhance survivors' access to justice when perpetrators exploit jurisdictional gaps.

VIII. CONCLUSION

Legal frameworks protecting survivors of domestic violence in the digital age have undergone remarkable evolution, transitioning from laws designed for pre-internet violence to comprehensive statutes addressing technology-facilitated abuse. The 2022 VAWA Reauthorization Act's definition of technological abuse, the 2025 Take It Down Act's criminalization of non-consensual intimate image distribution, and state-level coercive control legislation represent significant progress toward recognizing digital violence as serious harm requiring legal intervention.

However, persistent implementation challenges—including law enforcement training deficits, jurisdictional complexities, platform accountability gaps, and victim-blaming narratives—demonstrate that legislative reform alone proves insufficient. Effective protection requires sustained investment in specialized training, platform regulation addressing design features enabling abuse, survivor-centered legal remedies prioritizing victims' safety and autonomy, and international cooperation frameworks managing cross-border digital violence.

As technology continues evolving, legal frameworks must remain adaptive, anticipating emerging forms of abuse rather than reacting after harm occurs. The rise of artificial intelligence, virtual reality, and increasingly sophisticated surveillance technologies portends new mechanisms for control and harassment. Policymakers must engage technologists, survivors, advocates, and legal scholars in ongoing dialogue ensuring that laws protect fundamental rights to safety, privacy, and dignity in digital spaces.

Ultimately, addressing technology-facilitated domestic violence requires recognizing that digital and physical abuse constitute interconnected manifestations of gendered violence rooted in patriarchal power structures. Legal frameworks protecting survivors must therefore integrate technical solutions with broader efforts challenging cultural norms normalizing violence against women, promoting digital literacy and safety education, and fostering social conditions where all individuals can live free from fear, control, and harassment—whether experienced through physical force or digital technologies.

REFERENCES

- Bond, E., & Tyrrell, K. (2021). Understanding revenge pornography: A national survey of police officers and staff in England and Wales. *Journal of Interpersonal Violence*, 36(5–6), 2166–2181. <https://doi.org/10.1177/0886260518760011>
- Centers for Disease Control and Prevention. (2024). *Intimate partner violence*. U.S. Department of Health and Human Services.
- Commonwealth of Massachusetts. (2024). *An Act to prevent abuse and exploitation* (H.4744). Massachusetts Legislature.
- Domestic Violence Services Network. (2024). October 2024: A legal leap forward—MA's new coercive control law. *DVSN News and Updates*. <https://www.dvsn.org/october-2024-a-legal-leap-forward-mas-new-coercive-control-law/>
- Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *British Journal of Criminology*, 59(3), 551–570.
- Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: Domestic violence and the competing roles of digital media platforms. *Feminist Media Studies*, 18(4), 609–625.
- Franks, M. A. (2023). *The cult of the Constitution: Our deadly devotion to guns and free speech*. Stanford University Press.
- Freed, D., Palmer, J., Minchala, D. E., Levy, K., Ristenpart, T., & Dell, N. (2018). A stalker's paradise: How intimate partner abusers exploit technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems* (pp. 1–13). Association for Computing Machinery.
- Harris, B. A., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *British Journal of Criminology*, 59(3), 530–550.
- McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. *Feminist Legal Studies*, 25(1), 25–46.
- Pence, E., & Paymar, M. (1993). *Education groups for men who batter: The Duluth model*. Springer Publishing Company.
- Powell, A., & Henry, N. (2019). Technology-facilitated sexual violence victimization: Results from an online survey of Australian adults. *Journal of Interpersonal Violence*, 34(17), 3637–3665.
- Stark, E. (2007). *Coercive control: How men entrap women in personal life*. Oxford University Press.
- Take It Down Act, S. 146, 119th Cong. (2025).
- Violence Against Women Act of 1994, Pub. L. No. 103-322, tit. IV, 108 Stat. 1902 (1994).
- Violence Against Women Act Reauthorization Act of 2022, Pub. L. No. 117-103, div. W, 136 Stat. 49 (2022).
- Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960 (2006).
- Violence Against Women Reauthorization Act of 2013, Pub. L. No. 113-4, 127 Stat. 54 (2013).