



Digital Safety and Privacy Risks in Intimate Partner Violence Disclosures: Platform Governance and Survivor Protection

Susan Page

University of Tulsa, Tulsa, Oklahoma.

ABSTRACT :

The increasing integration of social media into everyday communication has transformed how individuals disclose experiences of intimate partner violence (IPV), seek assistance, and access support networks. Although digital platforms provide opportunities for survivor empowerment, public awareness, and community engagement, they also introduce significant safety, privacy, and ethical challenges. This study examines digital safety and privacy risks associated with IPV disclosures, emphasizing platform governance mechanisms and survivor protection strategies. It explores how unauthorized information sharing, digital surveillance, cyberstalking, identity exposure, algorithmic amplification, and technology-facilitated abuse can intensify survivor vulnerability. Particular attention is given to privacy controls, content moderation policies, reporting mechanisms, data governance practices, and institutional accountability in managing sensitive disclosures. The study further considers how gender inequalities, cultural contexts, digital literacy, and unequal access to protective technologies influence disclosure experiences and safety outcomes. By integrating survivor-centered perspectives with digital governance principles, the research proposes a conceptual framework for strengthening platform responsibility, trauma-informed moderation, confidential reporting, and accessible safety interventions. Ultimately, it contributes to understanding how digital environments can support safer disclosures while protecting survivor autonomy, dignity, and fundamental privacy rights.

Keywords: Intimate Partner Violence; Digital Safety; Privacy Risks; Social Media Disclosure; Platform Governance; Survivor Protection.

1. INTRODUCTION

1.1 Digital Communication and the Transformation of Personal Disclosure

The rapid expansion of social media, online communities, instant messaging applications, and interconnected digital technologies has transformed interpersonal communication and personal information disclosure [1]. Digital platforms increasingly facilitate public expression of sensitive experiences, enabling individuals to communicate personal narratives beyond traditional geographical and social boundaries [2]. These environments provide opportunities for emotional expression, collective awareness, peer engagement, and access to institutional assistance, particularly when conventional support systems are inaccessible or unresponsive [3]. However, the accessibility and persistence of digital information introduce complex questions concerning confidentiality, consent, and individual control over personal narratives [4]. Consequently, digital connectivity simultaneously strengthens opportunities for self-expression and creates vulnerabilities associated with information dissemination, audience unpredictability, and privacy violations [5]. Understanding these competing dynamics is essential for evaluating disclosure practices involving sensitive interpersonal experiences [6].

1.2 Intimate Partner Violence Disclosure in Digital Environments

Intimate partner violence (IPV) encompasses physical aggression, sexual violence, psychological abuse, coercive control, and technology-facilitated behaviors occurring within current or former intimate relationships [2]. Survivors may disclose abusive experiences through social media posts, anonymous discussion forums, private messaging groups, or specialized digital support communities to obtain emotional validation, practical guidance, and social recognition [7]. Such disclosures can facilitate peer solidarity, strengthen awareness of abusive relationships, and connect individuals with counseling, advocacy organizations, and protective services [4]. Digital anonymity may also reduce perceived barriers associated with stigma, geographical isolation, and fear of judgment [8]. Nevertheless, disclosure decisions frequently involve competing considerations of personal autonomy, emotional readiness, audience trust, and physical security [3]. Information initially shared within supportive environments may circulate beyond intended audiences, exposing survivors to unwanted identification, retaliation, or renewed psychological distress [6].

1.3 Emerging Digital Safety and Privacy Challenges

Despite their supportive potential, digital disclosure environments expose IPV survivors to interconnected safety and privacy threats, including cyberstalking, unauthorized surveillance, identity exposure, retaliatory harassment, and nonconsensual redistribution of sensitive information [5].

Platform architectures can intensify these vulnerabilities through algorithmic content amplification, persistent data storage, searchable communication histories, and interconnected social networks [1]. Consequently, disclosures intended for restricted audiences may become accessible to perpetrators, acquaintances, or hostile online communities [7]. Inadequate privacy controls, inconsistent content moderation, complicated reporting procedures, and delayed responses to harmful content can further undermine survivor protection [8]. These challenges demonstrate that digital safety cannot depend exclusively on individual privacy decisions or technological literacy [4]. Instead, effective protection requires institutional accountability, risk-sensitive platform design, transparent governance mechanisms, and coordinated responses that recognize the distinctive vulnerabilities associated with IPV disclosures [6].

1.4 Research Problem, Objectives, and Article Organization

Existing scholarship addresses digital IPV disclosures, technology-facilitated abuse, information privacy, and platform accountability, yet these perspectives are frequently examined independently, limiting integrated understanding of survivor protection [3]. This conceptual fragmentation complicates the identification of governance responsibilities and effective safeguards across diverse digital environments [7]. Accordingly, this article pursues three objectives: identifying principal digital safety and privacy risks associated with IPV disclosures [1]; critically evaluating platform governance and institutional accountability mechanisms [5]; and developing an integrated survivor-centered protection framework [8]. The analysis combines disclosure theory, digital privacy principles, sociotechnical risk assessment, and governance perspectives [2]. Subsequent sections examine theoretical foundations, emerging vulnerabilities, institutional safeguards, protection strategies, policy implications, and future research priorities.

2. CONCEPTUAL AND THEORETICAL FOUNDATIONS

2.1 Intimate Partner Violence, Disclosure Decisions, and Survivor Agency

Intimate partner violence disclosure represents a context-dependent process shaped by personal safety, relational dynamics, cultural expectations, and access to supportive institutions [6]. Survivors may disclose abusive experiences to seek emotional reassurance, practical assistance, or recognition of previously concealed harm [8]. However, stigma, anticipated disbelief, economic dependence, and fear of retaliation can discourage disclosure or influence the selection of trusted audiences [7]. Digital environments complicate these decisions because information initially communicated within restricted networks may subsequently reach unintended recipients [9]. Survivor agency therefore requires meaningful control over disclosure timing, content, audience, and subsequent information sharing [10]. Importantly, survivor-initiated disclosure differs fundamentally from unauthorized exposure by third parties, which may undermine consent and intensify vulnerability [11]. Understanding these distinctions establishes autonomy, contextual sensitivity, and informed decision-making as essential principles for evaluating digital disclosure practices and protective interventions [12].

2.2 Communication Privacy Management and Digital Boundary Regulation

Communication Privacy Management theory provides a conceptual foundation for examining how individuals establish, negotiate, and maintain boundaries surrounding sensitive personal information [9]. The theory emphasizes privacy ownership, information co-ownership, and coordinated expectations governing subsequent disclosure [11]. Within digital environments, survivors may share experiences with selected audiences while expecting recipients to respect confidentiality and established communication boundaries [13]. However, screenshots, reposting, algorithmic redistribution, and persistent digital archives can destabilize these expectations by transferring information beyond its intended context [8]. Such boundary turbulence becomes particularly consequential when sensitive disclosures reveal personal identities, locations, relationships, or experiences of abuse [10]. Unauthorized redistribution may facilitate perpetrator identification, retaliatory behavior, and renewed psychological distress [12]. Consequently, digital privacy protection requires both interpersonal respect for disclosure boundaries and platform mechanisms supporting audience control, consent management, and information confidentiality [7].

2.3 Technology-Facilitated Abuse and Sociotechnical Vulnerability

Technology-facilitated abuse encompasses harmful behaviors conducted through digital devices, communication platforms, surveillance applications, and networked information systems to intimidate, monitor, manipulate, or control intimate partners [10]. Such practices may extend existing patterns of coercive control through unauthorized account access, location monitoring, impersonation, threatening communications, and nonconsensual information dissemination [6]. Sociotechnical perspectives emphasize that these harms emerge through interactions between technological affordances, interpersonal power inequalities, and institutional protection mechanisms [12]. Platform features enabling persistent visibility, rapid content redistribution, and interconnected user identification may unintentionally increase opportunities for exploitation [9]. Vulnerability also varies according to economic resources, digital literacy, disability, geographical isolation, and access to trusted support services [13]. Accordingly, technology-facilitated abuse cannot be understood exclusively as individual misconduct; its prevention also requires attention to platform architecture, structural inequalities, and institutional accountability [8].

2.4 Platform Governance, Digital Rights, and Survivor-Centered Safety

Platform governance encompasses technical safeguards, institutional policies, content moderation procedures, reporting mechanisms, and accountability arrangements regulating digital interactions [11]. Within IPV disclosure environments, effective governance requires integrating privacy-by-design and

safety-by-design principles into platform development and operational decision-making [7]. These principles emphasize data minimization, accessible privacy controls, informed consent, risk-sensitive moderation, and mechanisms for preventing unauthorized information exposure [13]. Trauma-informed governance additionally recognizes survivors' vulnerability, prioritizing confidentiality, respectful communication, procedural transparency, and avoidance of secondary victimization [9]. Digital rights concerning privacy, expression, autonomy, and access to remedies provide complementary foundations for institutional responsibility [12]. Collectively, these perspectives establish a conceptual relationship in which disclosure circumstances influence privacy vulnerabilities, technological affordances shape potential harms, and governance interventions mediate survivor protection outcomes [10]. This integrated foundation informs the subsequent assessment of digital risks and institutional safeguards.

3. DIGITAL SAFETY AND PRIVACY RISKS IN IPV DISCLOSURES

3.1 Unauthorized Disclosure, Identity Exposure, and Information Persistence

Unauthorized disclosure represents a significant privacy threat when intimate partner violence (IPV) survivors' personal narratives, photographs, communications, or identifying information are disseminated without informed consent [12]. Digital practices such as doxxing, screenshot circulation, unauthorized reposting, and content redistribution can extend sensitive information beyond its intended audience [14]. The searchable and persistent nature of online content further complicates information removal, particularly when disclosures are replicated across interconnected platforms [16]. Even seemingly anonymous accounts may become identifiable through contextual details, social connections, location references, or previously published information [13]. Such exposure may facilitate perpetrator retaliation, unwanted contact, reputational damage, and threats to personal security [17]. Furthermore, survivors experiencing unauthorized redistribution may withdraw from supportive communities, restrict future disclosures, or lose confidence in digital assistance mechanisms [15]. These vulnerabilities demonstrate the importance of confidentiality safeguards, audience restrictions, and survivor-controlled information management throughout disclosure processes [18].

3.2 Digital Surveillance, Cyberstalking, and Technology-Facilitated Coercive Control

Digital surveillance and cyberstalking extend coercive control into technologically mediated environments, allowing perpetrators to monitor survivor activities, communications, and interpersonal relationships [13]. Common mechanisms include unauthorized account access, location tracking, device compromise, impersonation, password exploitation, and persistent monitoring of social media interactions [15]. Information obtained through digital disclosures may reveal daily routines, support networks, or geographical locations, potentially facilitating intimidation and retaliatory behavior [17]. Platform connectivity can intensify these threats by linking personal profiles, contact networks, photographs, and location-associated information across services [14]. Importantly, interpersonal surveillance differs from platform-level data processing: the former involves abusive monitoring or exploitation by individuals, whereas the latter concerns institutional collection, retention, and analysis of user information [18]. Nevertheless, weak authentication controls, excessive information visibility, and inadequate security procedures may create opportunities for both forms of exposure [16]. Effective prevention therefore requires secure account management, contextual privacy protections, accessible safety guidance, and coordinated institutional responses to technology-facilitated coercion [19].

3.3 Algorithmic Amplification, Harassment, and Secondary Victimization

Algorithmic recommendation systems may amplify sensitive IPV disclosures when platform ranking mechanisms prioritize engagement, interaction frequency, or perceived content relevance [14]. Although increased visibility can facilitate awareness and supportive responses, it may also expose survivors to unintended audiences, hostile communities, and perpetrators [16]. Online harassment, victim blaming, stigmatizing commentary, coordinated abuse, and threatening communications can subsequently transform disclosure environments into spaces of secondary victimization [18]. Repeated circulation of traumatic narratives may intensify emotional distress, undermine perceived social support, and reduce survivors' control over personal experiences [12]. Automated moderation systems may additionally misinterpret disclosure contexts, potentially restricting legitimate survivor testimony while failing to identify harmful interactions [17]. These concerns illustrate the limitations of engagement-oriented platform governance when safety considerations remain insufficiently integrated into content distribution practices [15]. Risk-sensitive amplification controls, contextual moderation, and accessible reporting mechanisms are therefore essential for reducing unintended exposure and protecting survivor dignity [19].

3.4 Data Collection, Retention, and Third-Party Privacy Vulnerabilities

Digital platforms routinely process personal information through account registration, behavioral monitoring, interaction tracking, and automated profiling, creating additional privacy concerns for survivors disclosing IPV experiences [15]. Disclosure-related metadata, including timestamps, interaction histories, device identifiers, and location-associated records, may reveal sensitive patterns even when explicit identifying information is withheld [17]. Extended data retention and third-party information sharing can increase exposure risks, particularly where privacy notices lack clarity or meaningful consent mechanisms [19]. Inadequate access restrictions, insecure integrations, and insufficient oversight of external data processors may further compromise confidentiality [13]. These vulnerabilities are especially consequential when digital records reveal survivor relationships, support-seeking activities, or potential safety arrangements [16]. Consequently, effective governance requires data minimization, purpose limitation, proportionate retention, secure processing, and transparent accountability procedures [18]. Strengthening these safeguards can preserve survivor autonomy, reinforce institutional trust, and reduce opportunities for unauthorized information exploitation [14].

3.5 Intersectional Vulnerabilities and Unequal Digital Safety Outcomes

Digital safety risks are not experienced uniformly, as gender inequalities, disability, socioeconomic circumstances, age, cultural expectations, and geographical location influence survivors' technological resources and protection opportunities [16]. Individuals facing social marginalization may encounter additional barriers involving language accessibility, institutional discrimination, limited connectivity, and restricted access to confidential support services [18]. Survivors with limited digital literacy may experience difficulties configuring privacy settings, identifying compromised accounts, or navigating complicated reporting procedures [12]. Similarly, economic dependence and shared-device arrangements may constrain opportunities for secure communication and independent technology use [19]. Cultural stigma and concerns about community recognition can further intensify the consequences of unintended disclosure [15]. These intersecting vulnerabilities demonstrate that standardized safety mechanisms may inadequately address diverse survivor circumstances [17]. Effective protection therefore requires accessible interfaces, multilingual assistance, context-sensitive safeguards, and survivor-informed governance strategies that accommodate unequal technological and institutional resources [13].

Table 1. Classification of Digital Safety and Privacy Risks Associated with IPV Disclosures

Risk Category	Principal Mechanism	Potential Survivor Consequence	Protection Priority
Identity exposure	Unauthorized information sharing, doxxing, and reposting	Identification, retaliation, and loss of confidentiality	Confidentiality controls and restricted information sharing
Digital surveillance	Account monitoring, location tracking, and unauthorized access	Coercive control, intimidation, and personal safety threats	Account protection, device security, and authentication safeguards
Algorithmic amplification	Automated content ranking and increased disclosure visibility	Harassment, unwanted exposure, and perpetrator identification	Audience restrictions and risk-sensitive visibility controls
Data privacy violations	Excessive data collection, retention, and third-party disclosure	Loss of confidentiality and unauthorized information exploitation	Data minimization, access restrictions, and retention controls
Online victimization	Harassment, victim blaming, stigmatization, and coordinated abuse	Psychological distress, withdrawal from support, and secondary victimization	Trauma-informed moderation and confidential reporting
Unequal digital protection	Accessibility limitations, resource inequalities, and institutional barriers	Disproportionate vulnerability and reduced access to protective services	Inclusive interfaces, multilingual support, and accessible safety mechanisms

4. PLATFORM GOVERNANCE AND INSTITUTIONAL ACCOUNTABILITY

4.1 Privacy Policies, Consent Management, and Data Governance

Platform privacy policies establish institutional expectations regarding personal information collection, processing, retention, and disclosure, yet conventional approaches may inadequately address the heightened vulnerabilities associated with intimate partner violence (IPV) disclosures [19]. Standardized privacy notices frequently employ complex terminology, broad processing permissions, and fragmented consent arrangements that limit meaningful user understanding [21]. For survivors, insufficiently transparent information practices may expose sensitive narratives, interaction histories, and identifying metadata to unintended recipients [23]. Effective governance therefore requires informed consent, purpose limitation, data minimization, restricted access, and proportionate retention periods [20]. Nevertheless, user-controlled privacy settings may provide limited protection when platform defaults encourage visibility or when perpetrators possess unauthorized account access [25]. Privacy-by-design principles offer an alternative by embedding confidentiality safeguards, granular disclosure permissions, and secure processing throughout platform development [22]. Such arrangements should prioritize survivor autonomy while ensuring that privacy protections remain accessible, understandable, and responsive to evolving safety circumstances [24].

4.2 Content Moderation, Reporting Mechanisms, and Harmful Content Removal

Content moderation and reporting mechanisms constitute essential institutional responses to harassment, impersonation, threats, doxxing, and unauthorized dissemination of IPV-related information [20]. However, automated detection limitations, delayed intervention, inconsistent policy enforcement, and inaccessible appeals may weaken their protective effectiveness [22]. Survivors navigating complicated reporting systems may experience repeated exposure to harmful content or additional emotional distress when required to reproduce traumatic experiences [24]. Trauma-informed moderation therefore requires confidential reporting pathways, appropriately trained reviewers, clear communication, and procedures minimizing unnecessary disclosure [26]. Platforms should additionally provide accessible escalation mechanisms for urgent safety concerns while preserving meaningful opportunities to challenge inaccurate decisions [21]. Importantly, harmful content removal must be distinguished from suppressing survivor-controlled testimony, particularly when disclosures serve advocacy, documentation, or support-seeking purposes [23]. Context-sensitive moderation should consequently balance protection against retaliation with survivor autonomy, procedural fairness, and the preservation of legitimate expression [27].

4.3 Algorithmic Accountability and Safety-Oriented Platform Design

Algorithmic recommendation, content ranking, and automated moderation increasingly shape the visibility, circulation, and accessibility of sensitive online disclosures [21]. Engagement-oriented systems may unintentionally amplify IPV narratives beyond intended audiences, increasing opportunities

for harassment, identification, and retaliatory interactions [23]. Similarly, automated moderation may inadequately distinguish survivor testimony from abusive communications when contextual understanding remains limited [25]. Safety-oriented platform design therefore requires risk-sensitive recommendation controls, customizable visibility restrictions, and mechanisms for reducing harmful amplification [27]. Algorithmic impact assessments can support identification of foreseeable disclosure-related risks before and after system deployment [20]. Transparency concerning ranking practices, moderation decisions, and available protective controls is equally important for informed participation [24]. Nevertheless, automated safeguards should remain proportionate and subject to meaningful human oversight, ensuring that interventions do not unnecessarily restrict survivor expression or undermine individual autonomy [26].

4.4 Regulatory Responsibilities and Cross-Jurisdictional Protection Challenges

Regulatory frameworks governing data protection, online safety, and technology-facilitated abuse establish important institutional obligations concerning personal information security and harmful digital conduct [22]. Principles reflected in instruments such as the General Data Protection Regulation emphasize lawful processing, data minimization, transparency, and accountability [24]. However, jurisdictional differences in privacy protections, intermediary responsibilities, reporting obligations, and enforcement mechanisms complicate consistent survivor protection [26]. Cross-border platform operations may further create uncertainty regarding applicable legal standards, information-sharing procedures, and access to remedies [19]. These challenges become particularly significant when survivors, perpetrators, digital service providers, and stored information are situated across different jurisdictions [25]. Effective regulatory responses therefore require coordinated oversight, proportionate compliance mechanisms, and accessible institutional remedies [27]. Nevertheless, formal legal compliance should not be equated with comprehensive survivor safety, since emerging technological threats may exceed existing regulatory protections [23].

4.5 Institutional Accountability, Transparency, and Governance Evaluation

Institutional accountability requires digital platforms to identify foreseeable disclosure-related harms, implement proportionate safeguards, and respond effectively when protection mechanisms fail [23]. Independent safety audits, transparent enforcement reporting, accessible appeals, and documented corrective actions can strengthen governance credibility [25]. Evaluation should extend beyond policy existence to examine operational responsiveness, confidentiality protection, moderation consistency, and survivor experiences [27]. Relevant indicators include reporting resolution times, unauthorized exposure incidents, successful appeals, and accessibility of protective controls [21]. Survivor-informed assessments can additionally reveal institutional weaknesses that conventional compliance evaluations overlook [26]. However, monitoring procedures must avoid unnecessary collection of sensitive information or creating additional surveillance risks [20]. Integrating independent oversight, measurable performance indicators, and continuous policy improvement can support more trustworthy and survivor-responsive digital environments [24].

Table 2. Platform Governance Mechanisms and Their Implications for Survivor Protection

Governance Dimension	Protective Mechanism	Implementation Challenge	Evaluation Indicator
Privacy governance	Data minimization, encryption, restricted access, and retention controls	Complex information-sharing arrangements and inconsistent privacy defaults	Unauthorized exposure incidents and compliance with retention requirements
Consent management	Granular disclosure permissions and accessible consent controls	Limited user understanding and difficulties withdrawing consent	Consent-control usability and effectiveness of permission changes
Content moderation	Trauma-informed human review and contextual content assessment	Inconsistent moderation decisions, automated classification errors, and delayed responses	Response time, decision consistency, and resolution quality
Algorithmic accountability	Visibility restrictions, amplification safeguards, and algorithmic risk assessments	Opaque ranking systems and difficulties identifying harmful amplification	Harmful amplification frequency and documented risk mitigation
Reporting and appeals	Confidential escalation procedures, accessible reporting, and independent review	Retaliation concerns, procedural complexity, and accessibility barriers	Reporting completion rates, appeal outcomes, and resolution effectiveness
Institutional oversight	Independent safety assessments, transparent reporting, and corrective action procedures	Limited institutional transparency and inconsistent accountability	Audit findings, corrective action completion, and survivor-informed evaluations

5. SURVIVOR-CENTERED DIGITAL PROTECTION FRAMEWORK

5.1 Foundational Principles of Survivor-Centered Digital Protection

Survivor-centered digital protection requires an integrated approach prioritizing autonomy, confidentiality, informed consent, accessibility, and trauma-informed engagement throughout online disclosure processes [18]. Unlike conventional safety models emphasizing standardized restrictions, survivor-centered governance recognizes that individuals experience distinct threats, support needs, and disclosure preferences [20]. Meaningful autonomy requires control over information visibility, audience selection, reporting decisions, and participation in protective interventions [22]. Confidentiality safeguards

must additionally prevent unnecessary information exposure while maintaining accessible pathways to institutional assistance [19]. Trauma-informed practices should minimize secondary victimization by avoiding repetitive disclosure requirements, coercive interventions, and dismissive responses to reported abuse [24]. Importantly, excessive content restrictions may inadvertently silence survivor testimony or obstruct access to supportive communities [21]. Consequently, protective mechanisms should remain adaptable, proportionate, and responsive to individual circumstances. Survivor participation in platform design, governance assessment, and policy development is essential for ensuring that protective systems reflect lived experiences and evolving safety priorities [25].

5.2 Preventive Privacy and Security Safeguards

Preventive digital protection begins with privacy-preserving platform defaults, granular audience controls, secure authentication, and accessible account-management mechanisms [19]. These safeguards can reduce unintended exposure by enabling survivors to restrict disclosure visibility, manage information-sharing permissions, and review connected applications [21]. Optional pseudonymity, secure messaging, data minimization, and restricted metadata accessibility may further strengthen confidentiality [23]. Platforms should incorporate mechanisms for limiting unauthorized redistribution, including controlled sharing options, sensitive-information warnings, and procedures for addressing nonconsensual content circulation [20]. However, technical safeguards cannot guarantee complete protection because screenshots, external recording, and information replication may circumvent platform restrictions [25]. Additional vulnerabilities arise when perpetrators possess device access, account credentials, or control over shared communication infrastructure [18]. Consequently, preventive interventions should combine technological safeguards with accessible security guidance, discreet account recovery options, and individualized risk assessment. Effective implementation requires balancing protective functionality with usability, survivor autonomy, and the practical limitations of digital security technologies [22].

5.3 Trauma-Informed Reporting and Responsive Safety Interventions

Responsive digital protection requires confidential reporting mechanisms that accommodate the emotional, practical, and security concerns associated with IPV disclosures [20]. Survivors should be able to report threats, impersonation, doxxing, harassment, and unauthorized information sharing through accessible interfaces without repeatedly recounting traumatic experiences [22]. A survivor-sensitive escalation process should provide clear response expectations, discreet communication options, and access to appropriately trained human reviewers [24]. Reports involving credible threats or sensitive identifying information may require prioritized assessment and proportionate protective measures [19]. Importantly, content restriction decisions should consider survivor preferences, particularly when disclosed material serves documentation, advocacy, or support-seeking purposes [21]. Evidence preservation should remain voluntary where appropriate, securely managed, and subject to transparent retention limitations [23]. Platforms should additionally provide optional referrals to qualified support organizations without assuming that every survivor requires identical interventions. Such procedures can strengthen institutional responsiveness while minimizing secondary victimization, unnecessary disclosure, and further exposure to abusive interactions [25].

5.4 Integrated Platform Governance and Survivor Protection Architecture

An integrated survivor protection architecture should coordinate privacy controls, risk identification, confidential reporting, trauma-informed moderation, and institutional oversight within a unified governance structure [21]. Platform operators would maintain secure technical infrastructure, while dedicated safety teams would assess reported threats and coordinate proportionate interventions [23]. Privacy officers would oversee consent management, information access, retention practices, and compliance with applicable data protection obligations [18]. External support organizations could provide specialist guidance, survivor-informed training, and optional referral pathways where appropriate [25]. Operational feedback mechanisms should connect incident reporting, moderation outcomes, and privacy assessments to continuous policy refinement [20]. Importantly, information sharing between institutional actors must remain proportionate, authorized, and sensitive to confidentiality requirements [22]. The architecture should accommodate differences in platform functionality, organizational resources, and jurisdictional responsibilities while maintaining consistent commitments to survivor autonomy, accessibility, and accountability [24].

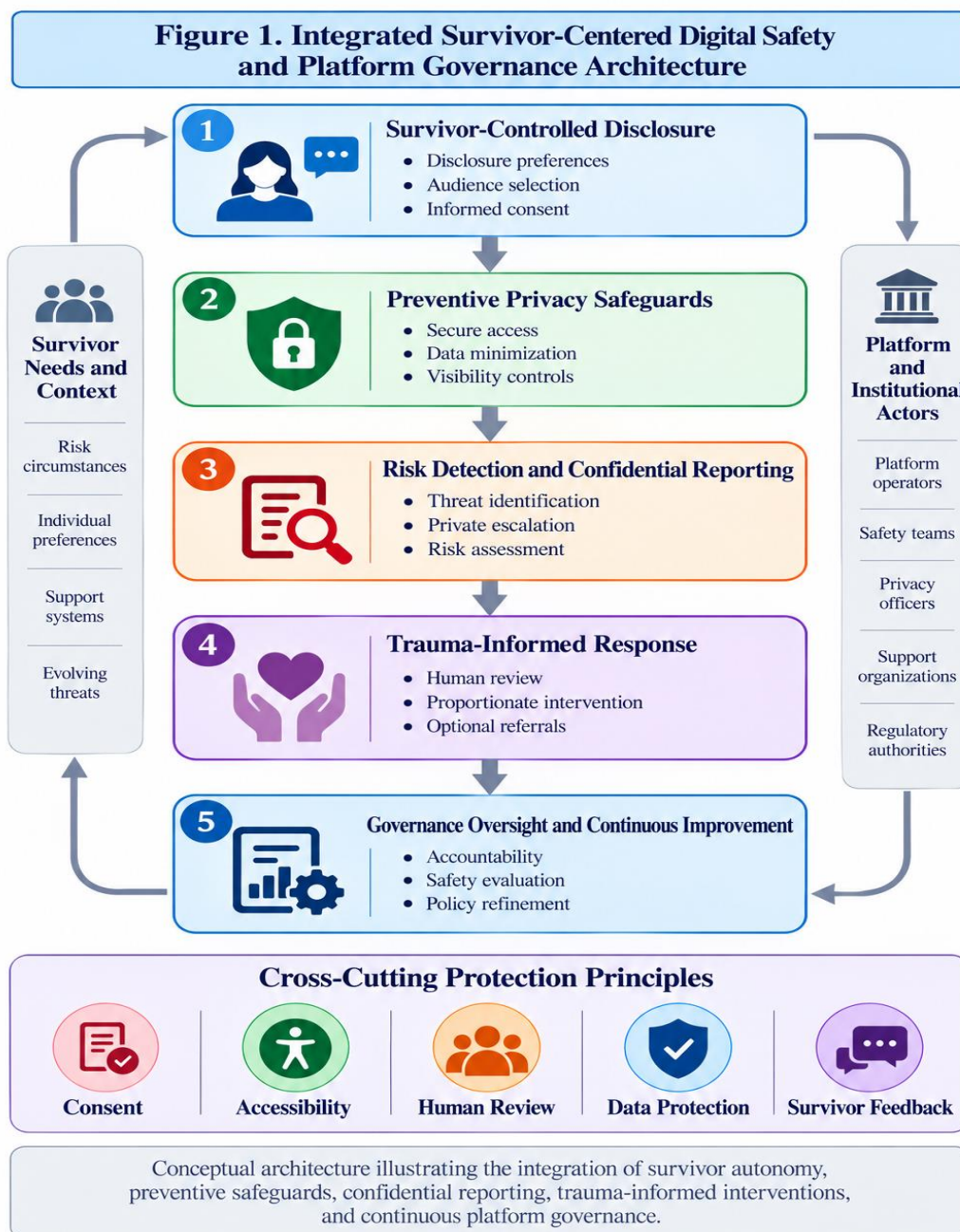


Figure 1. Integrated Survivor-Centered Digital Safety and Platform Governance Architecture

5.5 Protection Evaluation, Monitoring, and Continuous Improvement

Evaluating survivor-centered protection requires multidimensional indicators addressing reporting accessibility, institutional responsiveness, confidentiality safeguards, and intervention effectiveness [22]. Relevant measures include reporting completion rates, resolution times, unauthorized disclosure incidents, appeal outcomes, and accessibility performance [24]. Qualitative survivor feedback can complement operational indicators by identifying overlooked barriers, perceived safety concerns, and unintended consequences of protective interventions [19]. Periodic platform assessments should examine recurring vulnerabilities, moderation inconsistencies, and emerging technology-facilitated abuse patterns [21]. However, evaluation procedures must avoid excessive collection of sensitive information, intrusive monitoring, or mandatory disclosure of personal experiences [23]. Privacy-preserving assessment methods and voluntary participation can support meaningful oversight while respecting survivor autonomy [25]. Continuous improvement should consequently integrate evidence-based governance adjustments, specialist consultation, and transparent institutional accountability.

6. CRITICAL DISCUSSION AND POLICY IMPLICATIONS

6.1 *Balancing Disclosure Autonomy, Privacy, and Digital Safety*

Balancing survivor autonomy, information privacy, freedom of expression, and harm prevention represents a fundamental challenge in governing digital intimate partner violence disclosures [22]. Although restrictive moderation and automated content removal may reduce harmful exposure, excessive interventions can inadvertently suppress survivor testimony, limit advocacy, and undermine self-determination [24]. Digital safety therefore cannot be achieved exclusively through content deletion, particularly when sensitive information has already circulated across interconnected platforms [26]. Effective governance requires informed disclosure choices, configurable privacy settings, contextual risk assessment, and proportionate intervention mechanisms [23]. Survivors should retain meaningful influence over reporting decisions, information visibility, and available protective responses whenever circumstances permit [28]. Consequently, platform governance must reconcile institutional safeguarding responsibilities with individual agency, ensuring that protection measures minimize foreseeable harm without unnecessarily restricting legitimate expression or access to supportive communities [25].

6.2 *Implications for Platform Operators and Survivor Support Organizations*

Implementing survivor-centered digital protection requires platforms to strengthen accessible reporting interfaces, privacy-preserving architecture, specialist moderation, and confidential escalation procedures [23]. Collaboration with intimate partner violence support organizations can improve contextual understanding of coercive control, disclosure vulnerabilities, and trauma-informed intervention practices [25]. Digital safety practitioners may additionally contribute technical expertise concerning account compromise, surveillance prevention, and secure communication [27]. However, effective coordination requires clearly defined responsibilities, appropriate staff training, secure information-sharing arrangements, and survivor-informed operational protocols [29]. Smaller platforms may encounter financial, technological, and personnel constraints that complicate comprehensive implementation [24]. Accordingly, scalable governance strategies should prioritize essential safeguards while encouraging shared technical resources, specialist partnerships, and proportionate institutional oversight [26]. Sustainable implementation ultimately depends on integrating survivor protection into routine platform operations rather than treating disclosure-related harms as isolated moderation incidents [30].

6.3 *Regulatory and Policy Recommendations*

Regulatory responses should establish clearer institutional accountability expectations concerning sensitive disclosures, technology-facilitated abuse, unauthorized information dissemination, and foreseeable platform-related harms [24]. Risk-based governance frameworks can support proportionate obligations involving privacy protection, algorithmic assessment, accessible reporting, and timely intervention [26]. Independent safety evaluations and transparent moderation procedures may strengthen accountability while identifying persistent weaknesses in institutional practices [28]. Policymakers should additionally encourage data minimization, confidentiality safeguards, meaningful consent mechanisms, and accessible remedies for affected survivors [25]. Particular attention is necessary for individuals experiencing disability-related barriers, socioeconomic exclusion, linguistic disadvantages, or limited technological resources [27]. Because digital platforms operate across diverse legal environments, implementation should accommodate jurisdictional requirements without compromising fundamental protection principles [29]. Periodic regulatory review is essential for addressing emerging surveillance technologies, evolving abusive practices, and changing platform architectures [30].

6.4 *Research Limitations and Emerging Knowledge Gaps*

This conceptual analysis synthesizes theoretical perspectives and governance principles but does not establish the empirical effectiveness of proposed survivor protection mechanisms [25]. Differences in platform architecture, moderation policies, regulatory environments, and survivor circumstances may limit generalizability [27]. Further research should incorporate survivor-informed evaluations, participatory design, and comparative assessments of digital safety interventions [29]. However, collecting sensitive disclosure information raises substantial ethical challenges involving confidentiality, informed consent, participant security, and potential retraumatization [23]. Longitudinal investigations could examine changing disclosure risks, institutional responses, and protection outcomes across digital environments [28]. Cross-jurisdictional studies should additionally explore regulatory effectiveness and inequalities affecting marginalized survivor populations [30]. Such investigations would strengthen the evidence base for accountable, context-sensitive governance [26].

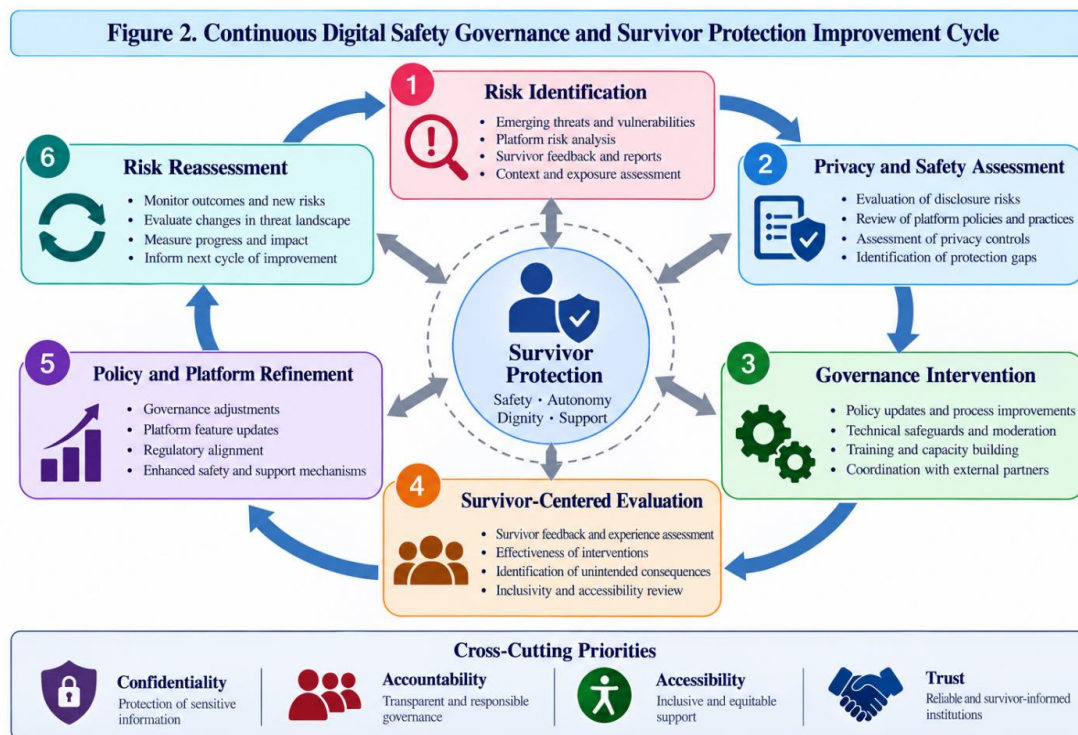


Figure 2. Continuous Digital Safety Governance and Survivor Protection Improvement Cycle

7. CONCLUSION AND FUTURE RESEARCH

7.1 Summary of Principal Findings and Conceptual Contributions

This article has examined the complex digital safety and privacy challenges associated with intimate partner violence disclosures, emphasizing unauthorized information sharing, digital surveillance, cyberstalking, algorithmic amplification, and technology-facilitated coercive control. The analysis demonstrates how disclosure practices interact with technological vulnerabilities, interpersonal power inequalities, and institutional governance deficiencies to influence survivor safety. Its principal conceptual contribution is an integrated survivor-centered governance framework connecting preventive privacy safeguards, confidential reporting, trauma-informed interventions, and continuous institutional accountability. By identifying major digital risks, evaluating platform governance mechanisms, and proposing coordinated protection strategies, the article addresses its central research objectives. The framework further emphasizes survivor autonomy, informed consent, accessibility, and proportional intervention as essential foundations for strengthening privacy protection and reducing disclosure-related harm across digital environments.

7.2 Practical and Policy Significance

The proposed framework offers practical implications for social media companies, digital safety professionals, intimate partner violence support organizations, and regulatory authorities. Platform operators should prioritize privacy-preserving design, accessible reporting mechanisms, trauma-informed moderation, and secure information management. Support organizations can strengthen survivor assistance through digital safety education, specialist referrals, and institutional collaboration. Policymakers should promote transparent governance, proportionate regulatory obligations, and accountability mechanisms addressing technology-facilitated abuse. Importantly, protective interventions must respect survivor autonomy while accommodating diverse accessibility requirements and individual safety circumstances. Continuous evaluation, independent oversight, and survivor-informed policy development remain essential for improving institutional responsiveness and sustaining trustworthy digital environments.

7.3 Future Research Directions and Concluding Perspective

Future research should empirically investigate survivor experiences, platform governance effectiveness, and the outcomes of digital protection interventions. Cross-platform comparisons, intersectional analyses, and longitudinal investigations could clarify how technological risks and institutional responses evolve across diverse populations and regulatory environments. Participatory research involving survivors should inform the development of accessible, context-sensitive safety mechanisms while maintaining rigorous ethical safeguards. Ultimately, survivor-centered governance provides an important foundation for advancing digital environments that protect privacy, preserve autonomy, strengthen accountability, and support safer intimate partner violence disclosures.

REFERENCE

1. Pentaraki M, Speake J. Technology-facilitated abuse within the context of intimate partner violence: Barriers to and recommendations for safety planning. *Human Geographies*. 2024 May 31;18(1).
2. Verma A, Asthana P. A Victimological and Legal Analysis of Gendered Cybervictimization and Protection of Women's Rights in Digital Space. In *Ethics, Justice, and Governance in the Age of AI and Digital Societies 2026* (pp. 205-246). IGI Global Scientific Publishing.
3. Hui V, Tian L, Feng X, Chen Q, Wong AK, Bloom TL. Perspectives and preferences of domestic violence survivors regarding digital platform and AI chatbot for help-seeking: A qualitative study. *PLoS One*. 2026 Feb 23;21(2):e0342453.
4. Al-Alosi H. Fighting fire with fire: Exploring the potential of technology to help victims combat intimate partner violence. *Aggression and Violent Behavior*. 2020 May 1;52:101376.
5. JN Chukwunweike, Moshood Yussuf, Oluwatobiloba Okusi, Temitope Oluwatobi Bakare, Ayokunle J. Abisola. The role of deep learning in ensuring privacy integrity and security: Applications in AI-driven cybersecurity solutions [Internet]. Vol. 23, *World Journal of Advanced Research and Reviews*. GSC Online Press; 2024. p. 1778–90. Available from: <https://dx.doi.org/10.30574/wjarr.2024.23.2.2550>
6. Alves Leitao R. *Technology-facilitated intimate partner abuse: Addressing the issue through codesign with survivors and support workers* (Doctoral dissertation, University of the Arts London).
7. Ifeanyi O, Akinjobi A. The Visibility-Safety Trade-off: A Multi-Layer Framework for Confidential Emergency Communication for Survivors of Intimate Partner Violence. Available at SSRN 7271918. 2026 Aug 10.
8. Ivy Nyantakyiwa Tsibuah. Allergen Management Readiness in University Dining Operations: Employee Knowledge, Attitudes, Practices, and Training Needs. *Archives of Current Research International*, 2026, 26 (9), pp.841-849. (hal-05754050)
9. Hearn J, Hall M, Lewis R, Niemistö C. The Spread of Digital Intimate Partner Violence: Ethical Challenges for Business, Workplaces, Employers and Management: J. Hearn et al. *Journal of Business Ethics*. 2023 Nov;187(4):695-711.
10. Mannan M, Youssef A, Mangeard P, Yu X, Tejaswi B, Pagey R. Privacy analysis of technologies used in intimate partner abuse. Technical Report. Concordia University, Montreal, CA. Retrieved 2024-02-13 from https://www.priv.gc.ca/en/opc-actions-and-decisions/research/funding-for-privacy-research-and-knowledge-translation/completed-contributions-program-projects/2022-2023/p_202223_11; 2023.
11. Ivy Nyantakyiwa Tsibuah. Effectiveness of Food-safety and Allergen Training among Food Handlers: A Systematic Review. *Current Journal of Applied Science and Technology*, 2026, 45 (9), pp.135-152. (hal-05731031)
12. Brown A, Harkin D, Tanczer LM. Safeguarding the “Internet of Things” for victim-survivors of domestic and family violence: Anticipating exploitative use and encouraging safety-by-design. *Violence against women*. 2025 Apr;31(5):1039-62.
13. Alebiosu O. Comparative analysis of public-private partnership legislation driving electricity infrastructure expansion, renewable energy investment, and economic resilience nationally. *Int J Foreign Trade Int Bus*. 2025;7(2):239-249. doi:10.33545/26633140.2025.v7.i2c.262.
14. Slupska J, Brown ML. Aiding intimate violence survivors in lockdown: Lessons about digital security in the Covid-19 pandemic. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts 2022* Apr 27 (pp. 1-5).
15. Tseng E, Freed D, Engel K, Ristenpart T, Dell N. A digital safety dilemma: Analysis of computer-mediated computer security interventions for intimate partner violence during covid-19. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems 2021* May 6 (pp. 1-17).
16. Grimani A, Gavine A, Moncur W. An evidence synthesis of covert online strategies regarding intimate partner violence. *Trauma, Violence, & Abuse*. 2022 Apr;23(2):581-93.
17. Kwaku Gyamfi Boamah. AI-Driven Threat Intelligence Adoption in Security Operations Centers: Human Skill Erosion or Analyst Augmentation? A Comparative Case Study of Resource-Constrained SOCs in Emerging Markets. *International Journal of Science and Research Archive*, 2026, 19(03), 025-033. Article DOI: <https://doi.org/10.30574/ijrsra.2026.19.3.1226>.
18. Cho K, Choi K, Park Y, Kim M, Kim S, Jeong D. DEF-IPV: A digital evidence framework for intimate partner violence victims. *Forensic Science International: Digital Investigation*. 2025 Oct 1;54:301979.
19. Eckstein JJ. To harm and heal: Digital disclosure and support-seeking for IPV victims. *Open Information Science*. 2021 Jan 1;5(1):175-89.
20. Moses LB, Breckenridge J, Gibson J, Lyons G. Technology-facilitated domestic and family violence: Protecting the privacy and safety of victim-survivors. *Law, technology and humans*. 2022 May 1;4(1):1-7.
21. Ivy Nyantakyiwa Tsibuah. Allergen Management Capacity and Training Gaps among School Nutrition Professionals: A Critical Narrative Review of Alignment with United States Department of Agriculture Professional Standards. *Current Journal of Applied Science and Technology*, 2026, 45 (10), pp.1-21. (hal-05738519)
22. Freed D, Palmer J, Minchala DE, Levy K, Ristenpart T, Dell N. Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. *Proceedings of the ACM on human-computer interaction*. 2017 Dec 6;1(CSCW):1-22.
23. Matthews T, O'Leary K, Turner A, Sleeper M, Woelfer JP, Shelton M, Manthorne C, Churchill EF, Consolvo S. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI conference on human factors in computing systems 2017* May 2 (pp. 2189-2201).
24. Kapur, I., Ravi, K., Eya, O. et al. Digital Disclosure of Intimate Partner Violence on Social Media: A Scoping Review. *J Fam Viol* (2026). <https://doi.org/10.1007/s10896-025-01039-0>
25. Bellini R, Lee K, Brown MA, Shaffer J, Bhalariao R, Ristenpart T. The {digital-safety} risks of financial technologies for survivors of intimate partner violence. In *32nd USENIX Security Symposium (USENIX Security 23)* 2023 (pp. 87-104).
26. Ivy Nyantakyiwa Tsibuah. Food Safety Knowledge, Attitudes and Hygiene Practices among Traditional Caterers in Urban Markets: A Critical Narrative Review with Implications for Market Circle, Takoradi, Ghana. *Journal of Scientific Research and Reports*, 2026, 32 (9), pp.485-504. (hal-05738702)
27. Khurana P. Digital Shadows: How Technology Is Reshaping the Reporting of Domestic Violence. *Scientific Journal of Artificial Intelligence and Blockchain Technologies (SJAIBT)*. 2025 Dec 3;2(4):1-1.
28. Hu Y, Gu YG. Breaking the silence in a “digital backstage”: A cyberfeminist analysis of Chinese women’s self-disclosure of intimate partner violence on social media. *Psychology of Violence*. 2026 Mar 26.
29. Emmanuel Uzoh. (2023). PREDICTIVE OPERATIONS INTELLIGENCE: AN AUTOMATED MACHINELEARNING SYSTEM FOR BOTTLENECK DETECTION AND DYNAMIC WORKSTREAM PRIORITIZATION IN SMALL AND MEDIUM-SIZED ENTERPRISES. *INTERNATIONAL JOURNAL OF ENGINEERING TECHNOLOGY RESEARCH & MANAGEMENT (IJETRM)*, 07(12), 793–806. <https://doi.org/10.5281/zenodo.22089397>

-
30. Poveda J, Lanter A, Antoniuk I, Mazurek ML, Freed D. "CHAT WITH ME below as if I were a human": Insights from Auditing AI Chatbots for Survivors of Domestic Violence. In The 2026 ACM Conference on Fairness, Accountability, and Transparency 2026 Jun 25 (pp. 1398-1423).