



The Digital Safeguard Centre

BY NANSEN.IO

Submission to the Second Action Plan Consultation
National Plan to End Violence against Women and Children 2022–2032
Submitted by The Digital Safeguard Centre

About The Digital Safeguard Centre

The Digital Safeguard Centre (formerly Nansen Digital Forensic Services) is an Australian centre working at the intersection of digital safety, domestic, family and sexual violence (DFSV), human rights and emerging technology. We are specialists in technology-facilitated abuse (TFA), providing TFA audits and digital safety assessments within DFSV support contexts. Our work integrates specialist technical capability with trauma-informed practice. Our practice includes assessing compromised devices and accounts, documenting findings to support safety planning and legal processes, and advising on remediation strategies for victim survivors.

The Digital Safeguard Centre also builds trauma-informed Artificial Intelligence (AI) tools applying frontline casework expertise and our specialist knowledge of the unique TFA threat landscape that strengthens victim-survivor safety and practitioner capability. Joliro is our signature platform, providing victim survivors with a safe and secure digital environment to remain connected with trusted family and friends, identify TFA risks and undertake structured, in-depth audits of their digital ecosystem in 21 languages. It also equips DFSV case managers with tools to support the identification, assessment and safe remediation of technology-related risks, strengthening contemporary responses to TFA.

Our commitment to evidence-based practice extends through a research partnership with the University of Canberra, including an embedded industry PhD program examining the effectiveness of current TFA interventions, methodologies and response models. We have also established what we describe as Australia's first TFA methodology lab to develop, evaluate and refine specialist approaches to identifying and responding to TFA.

Beyond frontline practice and research, the Digital Safeguard Centre contributes to national and international policy, standards and professional capability. We hold board-level representation at the Australian Risk Policy Institute and expert advisory roles with the Australian Computer Society, Standards Australia and the International Organization for Standardization (ISO).

Our work has been presented internationally, including at the United Nations Commission on the Status of Women (CSW70) and the University College London TFA Gender-Based Violence Conference 2026. We are an international partner of the Global Coalition Against Stalkerware and are establishing collaborative partnerships with DFSV organisations and universities in the United Kingdom. Within Australia, we support state governments through consultation and specialist industry training, and we develop the practical tools and methodologies that the sector increasingly relies on for TFA response and prevention.

This work has been recognised through two national 2024 AIIA iAwards (Not-for-Profit and Community Sector Solution of the Year, and the Inspiration Award for likely global impact), the 2024 InnovationAus Software Platform of the Year Award, the ACT Embracing Innovation category of the Telstra Best of Business Awards (national finalist), and the 2025 Technology for Good Award. Collectively, our

frontline practice, research, technology development and policy engagement provide the foundation for the recommendations contained in this submission.

Recognition should therefore be understood not as an exercise in terminology, but as a mechanism for strengthening public policy. Classification determines what governments measure, what services are expected to respond to, where funding is directed, how workforces are trained and where research investment occurs. A form of harm that lacks clear recognition within policy frameworks is less likely to receive sustained attention across each of these domains.

This submission proposes that distinct recognition should be considered where a form of abuse:

- creates identifiable harms not adequately addressed by existing categories,
- requires specialised professional capability and safety planning,
- creates governance gaps within existing policy settings,
- requires distinct legal, regulatory or industry responses, and
- would materially benefit from dedicated research, funding and accountability.

TFA satisfies each of these criteria, as demonstrated throughout this submission. Recognising TFA as a distinct category would not diminish the importance of other abuse forms, nor create a separate DFSV service system. Rather, it would strengthen existing responses by establishing nationally consistent definitions, embedding digital capability as a core workforce expectation, improving accountability, and ensuring Australia's DFSV framework evolves alongside the technologies that increasingly shape contemporary DFSV.

1. Technology has Changed the Architecture of Abuse

DFSV has never been a static concept. Over time, Australian governments have progressively broadened their understanding of abuse as research, practice and the lived experience of victim-survivors have demonstrated that violence extends beyond acts of physical assault. Behaviours once regarded as peripheral to the understanding of DFSV, including financial abuse, psychological abuse and patterns of coercive control, have come to be recognised because evidence established that existing frameworks did not adequately describe the harms experienced or support effective intervention.

Across Australia, victim-survivors increasingly live within interconnected digital environments. Smartphones synchronise with cloud accounts. Vehicles exchange location data via GPS and mobile applications. Smart home devices automate household functions. Wearable technologies record movement and health information. Families share photographs, calendars, passwords and locations through legitimate consumer platforms designed to encourage connectivity and convenience. These technologies have transformed daily life while simultaneously creating new opportunities for abuse.

Unlike many earlier forms of technology-enabled violence, contemporary TFA rarely depends upon sophisticated hacking or specialist technical expertise. It is more commonly embedded within ordinary consumer technologies that families use every day. Shared cloud accounts, location-sharing applications, digital identity platforms, family management tools and connected household devices have become integral to modern relationships. When relationships become abusive, these same technologies can be repurposed to facilitate surveillance, intimidation, manipulation and ongoing monitoring. Importantly, technology has not merely introduced new methods through which existing abuse is perpetrated, it has fundamentally altered the architecture within which abuse occurs.

Historically, many forms of DFSV relied upon physical proximity or repeated perpetrator action, and separation frequently disrupted opportunities for ongoing surveillance and control. Today, digital environments remain intact and accessible to perpetrators of abuse long after physical separation has occurred.

The emergence of generative artificial intelligence is accelerating this broader trend towards increasingly sophisticated forms of digital control. Capabilities that previously required significant technical knowledge are increasingly accessible to individuals without specialist expertise. Existing digital ecosystems, including cloud platforms, connected devices, location services and account management systems, already provide powerful mechanisms for surveillance, monitoring and control. Together, these developments are rapidly lowering the technical barriers to sophisticated digital abuse while increasing the complexity of identifying, investigating and responding to it.

The Digital Safeguard Centre's practice reflects this changing landscape. Through specialist digital safety audits conducted with victim-survivors of DFSV, our specialists increasingly encounter abuse that extends well beyond individual devices. Assessments routinely involve complex digital ecosystems comprising cloud platforms, shared accounts, online identities, wearable technologies, internet-connected devices and multiple third-party service providers. These environments frequently evolve over many years through legitimate sharing during relationships, making unauthorised access difficult to identify and complex to remediate safely.

This practical experience reflects a broader structural challenge for Australia's DFSV policy framework. Australia's understanding of DFSV has continued to evolve, yet the conceptual framework through which TFA is understood has remained comparatively unchanged. While technology itself has transformed dramatically, policy continues largely to characterise TFA as a means through which existing abuse categories are delivered. This submission argues that this approach no longer adequately reflects the nature of contemporary technology-enabled harm or provides a sufficient foundation for responding to it.

This transformation, rather than the mere presence of technology, is the central issue for policymakers. The rapid emergence of generative artificial intelligence is accelerating this transformation by lowering the technical barriers to increasingly sophisticated forms of TFA. As these capabilities become more accessible through consumer technologies, the gap between the rapidly evolving architecture of abuse and Australia's policy, legislative and service responses will continue to widen unless systems evolve at a comparable pace.

2. The Limits of the Current Policy Architecture

Australia has demonstrated a strong capacity to evolve its understanding of DFSV as evidence has revealed previously under-recognised forms of harm. However, the pace of technological change has created a growing gap between the environments in which abuse occurs, and the frameworks designed to prevent and respond to it.

The challenge is not that existing DFSV frameworks fail to recognise technology as relevant. Most contemporary definitions acknowledge that technology can be used to facilitate intimidation, harassment, surveillance, stalking, coercive control and other forms of abuse. This recognition has been an important and necessary first step. However, acknowledging that technology can be involved in abuse is not the same as recognising that technology has created distinct policy challenges requiring dedicated attention.

The distinction is significant. When TFA is understood primarily as a mechanism through which existing forms of violence are perpetrated, policy responses naturally focus on the abusive behaviour itself. While this remains essential, it may overlook the distinct characteristics of digital environments that enable, sustain and amplify abuse. These characteristics are set out below and demonstrate that digital environments have introduced new forms of persistence, complexity and interdependence that existing DFSV frameworks were not designed to fully address.

First, digital environments enable abuse to persist beyond physical separation. A perpetrator may no longer share a home with a victim-survivor, yet may continue to access shared accounts, monitor location information, view personal data, control connected devices or influence digital identities. Separation no longer necessarily creates the same interruption to surveillance and control that it historically provided in non-digital environments. Persistent digital connectivity enables abuse to continue across physical boundaries, allowing perpetrators to maintain access to information, accounts, devices and digital environments long after separation has occurred.

Second, TFA often involves digital systems and services that are controlled or administered by third parties rather than the victim-survivor or the perpetrator. Cloud platforms, telecommunications providers, government systems, application developers, smart device manufacturers and online service providers frequently hold information, administer account access or control digital services that are directly relevant to victim-survivor safety. Digital ecosystems mean that preventing and responding to DFSV increasingly requires the involvement of organisations that were never designed to be part of the DFSV response. This creates new governance, coordination and accountability challenges that are not adequately addressed within existing policy settings.

Third, TFA can operate at a scale, speed and reach that differs fundamentally from many other forms of DFSV. A compromised account can expose years of personal information. A location-sharing setting can continuously transmit a victim-survivor's whereabouts. A manipulated image or fabricated communication can be distributed instantly and potentially to global audiences, while digital impersonation can rapidly damage relationships, employment and reputation. Unlike many traditional forms of abuse, these harms can be replicated, amplified and disseminated almost instantaneously, creating risks that extend well beyond the original act. The speed, persistence and scalability of digital harm present challenges that traditional DFSV responses were not designed to address.

Fourth, TFA requires specialist technical capability that extends beyond traditional DFSV practice. Determining whether a device, account or broader digital environment has been compromised often requires expertise in digital systems, cloud platforms, account security and connected technologies. However, TFA presents challenges that are not always addressed through conventional cybersecurity models or approaches. Unlike many traditional cyber threats, TFA frequently involves perpetrators who previously held a trusted position within the victim-survivor's life and may have been legitimately granted access to devices, accounts or digital environments during the relationship. In these circumstances, TFA is often not characterised by an external actor breaching a security system. Rather, it may involve the misuse, retention or exploitation of legitimate access obtained through a relationship of trust. As a result, indicators of abuse may not resemble conventional technical compromise and may instead involve retained permissions, shared accounts, device connections or consumer technology settings that continue to provide access after the relationship or circumstances of trust have changed. Effective assessment therefore requires approaches that recognise the intersection between technical compromise and relationship dynamics. Equally, technical assessments undertaken without an understanding of coercive control, trauma-informed practice, safety planning and the lived experience of victim-survivors may fail to identify relevant risks or may inadvertently compromise safety. Effective responses require more than technical expertise alone. Digital safety assessments must integrate specialist

technical knowledge with an understanding of domestic and sexual violence, trauma-informed practice, safety planning and victim-survivor experiences.

Collectively, these characteristics demonstrate that technology is no longer simply a tool through which existing forms of abuse are perpetrated. Digital environments have become an additional domain in which abuse is planned, executed, sustained and experienced; one that extends well beyond Australia's existing DFSV framework and requires the dedicated policy attention set out in Section 4.

3. Policy and Service System Implications

The current policy architecture creates several significant challenges:

(i) Lack of Nationally Consistent Recognition and Definition

Without formal recognition of TFA as a distinct category within DFSV policy frameworks, terminology, data collection and service responses remain inconsistent. Different sectors may use different concepts, including cyber abuse, technology-facilitated coercive control, digital abuse, online abuse or technology-facilitated violence. While these terms often overlap, inconsistency limits the ability to measure prevalence, compare outcomes and develop nationally coordinated responses. Clear recognition within national policy settings would establish a foundation for consistent definitions, improved data collection and coordinated action across jurisdictions.

(ii) Workforce Capability Gaps

TFA is now a routine feature of many DFSV presentations, yet digital safety capability remains uneven across the sector. Practitioners are increasingly expected to identify technology risks, support account security, understand connected devices, assess digital surveillance concerns and provide safe technology advice. These expectations have expanded rapidly without corresponding investment in training, specialist roles or sustainable practice resources.

Building on the distinction outlined in Section 3, a future-focused TFA capability model should separate foundational digital safety capability, expected across the DFSV workforce, from specialist capability available through referral. Foundational capability should enable practitioners to identify digital safety risks, incorporate technology into risk assessment and safety planning, provide safe initial advice and recognise when specialist assistance is required. Specialist TFA capability should support structured digital safety assessments, analysis of account and device security, identification of persistent access pathways, review of connected technologies, preservation of digital evidence and safe remediation planning that accounts for the risks of separation.

Australia therefore requires a coordinated capability model supported by nationally consistent competency standards, accessible specialist referral pathways, practitioner support mechanisms and appropriate technical assessment resources. Digital safety should be embedded within contemporary DFSV practice, with TFA responses supported by dedicated specialist capability or tools, rather than general workforce training alone.

(iii) Uneven Impact Across Diverse Communities

TFA does not affect all victim-survivors equally. Aboriginal and Torres Strait Islander women, who are significantly overrepresented among victim-survivors of DFSV more broadly, also face particular barriers to safe engagement with digital safety assessment and remediation, including geographic isolation, distance from specialist services, and the compounding impact of colonisation and systemic racism on trust and help-seeking. Migrant and refugee women, women with disability, and LGBTIQ+ people can likewise face distinct and compounding barriers to accessing specialist digital safety support, including language barriers, reliance on family members for technology access, and services that are not designed around their specific circumstances. A national TFA response framework must be designed and delivered in partnership with these communities, drawing on culturally safe, trauma-informed and self-determined approaches, rather than assuming a single pathway to digital safety support will meet the needs of all victim-survivors. Unless TFA is recognised as a distinct and pervasive form of abuse, efforts to address it within these communities are unlikely to achieve meaningful impact.

(iv) TFA Affecting Children and Young People in Their Own Right

TFA is not confined to adult intimate partner contexts. Children and young people increasingly experience TFA in their own right, including image-based abuse and deepfakes generated by peers, harassment and exploitation through dating and social platforms, and the use of family devices, shared accounts or location-sharing tools by a parent to monitor or control a young person during and after parental separation. These experiences require developmentally appropriate, young person-centred approaches to digital safety assessment and support, distinct from adult-focused practice models. The Digital Safeguard Centre supports the recognition of children and young people as victim-survivors of TFA in their own right and recommends that any national digital safety capability and referral infrastructure be designed to meet their specific needs alongside those of adult victim-survivors.

4. Building a Future-Focused National Response

Recognising TFA as a distinct category provides an opportunity to strengthen existing responses rather than create a parallel system, ensuring TFA receives the same strategic attention, investment and accountability as other recognised forms of violence. Recognition should not make TFA the responsibility of specialist services alone. Rather, it embeds responsibility for identifying and responding to technology-related harm within mainstream DFSV practice, while ensuring specialist digital safety capability is available where advanced technical assessment and remediation are required.

The Digital Safeguard Centre recommends that Australia develop a national TFA response framework built upon the following principles.

(i) Establish National Recognition, Consistent Definitions and Measurement

TFA should be formally recognised within national DFSV policy frameworks. This recognition should include a nationally consistent definition that acknowledges TFA as:

- the use, misuse or exploitation of digital technologies, connected devices, online platforms or digital systems to monitor, control, intimidate, harass, impersonate, exploit or otherwise harm a victim-survivor, and
- a distinct category of DFSV that may intersect with, but is not limited to, coercive control, psychological abuse, stalking, financial abuse and other recognised forms of violence.

A consistent definition would support improved research, data collection, workforce development, service coordination and accountability across jurisdictions.

(ii) Embed Digital Safety as Core DFSV Practice

Digital safety should become an integrated component of DFSV response, rather than a specialist consideration only after technology concerns are identified. This requires:

- nationally consistent training standards,
- digital safety competencies within workforce frameworks,
- practical resources or tools for frontline practitioners,
- recognition that technology assessment is part of contemporary risk assessment and safety planning.

Every DFSV service should have access to appropriate digital safety capability, with foundational digital safety knowledge embedded across the workforce and specialist expertise available through established referral pathways where technology-related risks require specialist assessment, safe remediation or technical support. This will ensure technology-related risks are incorporated into contemporary DFSV assessment and safety planning.

(iii) Develop National Specialist Digital Safety Infrastructure

Australia requires a coordinated national capability to support victim-survivors and practitioners responding to TFA, including access to specialist expertise where technology-related risks require capabilities beyond general DFSV services. This should include:

- specialist digital safety assessment and remediation services,
- practitioner support and referral pathways,
- technical guidance resources,
- mechanisms for urgent assistance where digital compromise creates immediate safety risks, and
- consistent methodologies, frameworks and standards for digital safety assessment, risk identification and safe remediation.

Such capability should operate alongside existing DFSV services and be integrated into broader safety planning approaches. As set out in Section 4, this infrastructure must be designed in partnership with Aboriginal and Torres Strait Islander communities and other diverse population groups and must include developmentally appropriate pathways for children and young people experiencing TFA in their own right.

(iv) Strengthen Partnerships with Technology and Telecommunications Industries

The digital environments in which abuse occurs are increasingly governed by private companies and service providers. Effective prevention and response therefore requires meaningful engagement between government, specialist services and industry. Priority areas should include:

- safer account recovery processes,
- improved responses to DFSV-related account security issues,
- clearer pathways for ownership transfer of connected devices,
- improved privacy and safety-by-design principles,
- greater transparency regarding data access and device permissions.

Technology companies increasingly shape the conditions in which digital safety is either protected or compromised. They should therefore be recognised as key partners in preventing TFA.

(v) Invest in Research, Data and Evaluation

The absence of consistent national data on TFA limits Australia's ability to understand prevalence, emerging risks, service demand and effective interventions. Without reliable evidence, governments cannot accurately measure the scale of technology-facilitated harm, allocate resources effectively, evaluate responses or identify emerging risks. Investment is therefore required to establish:

- nationally consistent data collection and reporting mechanisms,
- longitudinal research into patterns, prevalence and impacts of TFA
- evaluation of prevention, intervention and response initiatives, and
- research into emerging technologies, including artificial intelligence and their implications for TFA.

(vi) Establish Safe and Ethical Frameworks for AI-Assisted Support

Building on the research priorities outlined in (v), a sixth and forward-looking principle addresses the safe integration of artificial intelligence into TFA responses. Increasingly, victim-survivors may turn to generative AI tools for information, reassurance or guidance about technology-related harm. While general-purpose AI systems may provide accessibility benefits and useful information, they are not specifically designed to undertake DFSV risk assessment, understand coercive control dynamics or provide trauma-informed responses. As a result, they may provide information that is inaccurate, incomplete or insufficiently tailored to a victim-survivor's safety context, which may inadvertently increase distress or contribute to unsafe decision-making.

At the same time, purpose-built AI systems developed specifically for family violence contexts have the potential to strengthen responses when designed within robust governance frameworks, informed by trauma-informed practice, specialist expertise and appropriate human oversight. The policy challenge is therefore not whether AI should be used, but how it can be safely, ethically and effectively integrated into family violence responses. Future policy settings should distinguish between general-purpose AI tools and specialist AI applications designed for family violence contexts, ensuring innovation occurs alongside appropriate safeguards, accountability and survivor-centred design.

5. Conclusion

Australia's DFSV framework has evolved because governments have recognised that harms previously overlooked require dedicated attention, investment and accountability. TFA represents the next stage of that evolution.

The central challenge is not that technology has merely created new tools through which existing forms of violence can be perpetrated. The challenge is that technology has transformed the environment in which abuse occurs. Digital systems now enable surveillance, control and harm to continue across physical boundaries, through persistent digital connections, automated processes and complex ecosystems involving multiple third parties. Australia's policy architecture must evolve at the same pace as the architecture of abuse.

Recognising TFA as a distinct category within DFSV policy frameworks is an essential step in achieving that objective. It will strengthen existing responses, improve accountability, build workforce capability and ensure that victim-survivors experiencing contemporary forms of harm receive responses that reflect the realities of their lives.

The question is no longer whether technology is relevant to DFSV. The question is whether Australia's policy framework has evolved to recognise that digital environments have become a new domain in which family violence is perpetrated.