A Taxonomy-Driven Case Study of Australian Web Resources Against Technology-Facilitated Abuse

Dipankar Srirag
d.srirag@unsw.edu.au
University of New South Wales
Sydney, Australia

Xiaolin Cen
xiaolin.cen@student.unsw.edu.au
University of New South Wales
Sydney, Australia

Rahat Masood
rahat.masood@unsw.edu.au
University of New South Wales
Sydney, Australia

Aditya Joshi
aditya.joshi@unsw.edu.au
University of New South Wales
Sydney, Australia

Abstract

Technology-Facilitated Abuse (TFA) encompasses a broad and rapidly evolving set of behaviours in which digital systems are used to harass, monitor, threaten, or control individuals. Although prior research has documented many forms of TFA, there is no consolidated framework for understanding how abuse types, prevention measures, detection mechanisms, and support pathways relate across the abuse life cycle. This paper contributes (i) a unified, literature-derived taxonomy of TFA grounded in a structured review of peer-reviewed studies, and (ii) the first large-scale, taxonomy-aligned audit of institutional web resources in Australia. We crawl 306 government, non-government, and service-provider domains, obtaining 52,605 pages, and classify each using hierarchical zero-shot models to map web content onto our taxonomy. Complementary emotion and readability analyses reveal how institutions frame TFA and how accessible their guidance is to the public. Our findings show that institutional websites cover only a narrow subset of harms emphasised in the literature, with approximately 70% of all abuse labelled pages focused on harassment, comments abuse, or sexual abuse, while less than 1% address covert surveillance, economic abuse, or long-term controlling behaviours. Support pathways are similarly limited, with most resources (62%) centred on digital information hubs rather than counselling, legal assistance, or community-based services. Readability analysis further shows that much of this content is written at late secondary or early tertiary reading levels (for example, ARI 18 to 22 across major categories), which may be inaccessible to a substantial portion of at-risk users. By highlighting strengths and gaps in Australia's support for TFA, our taxonomy and audit method provide a scalable basis for evaluating institutional communication, improving survivor resources, and guiding safer digital ecosystems across the Australian context. The taxonomy itself serves as a solid foundation for analyses in other national contexts to foster awareness regarding technology-facilitated abuse.

CCS Concepts

• **Security and privacy → Human and societal aspects of security and privacy**.

Keywords

Technology-Facilitated Abuse, Cyber Abuse, Digital Safety, Digital Harms, Human-Centred Security

1 Introduction

Technology-Facilitated Abuse (TFA) refers to the use of networked technologies such as smartphones, social media platforms, online services, and smart devices to harass, monitor, threaten, or control another person [9, 17]. While many abusive behaviours predate digital media, web-facilitated infrastructures have intensified their reach and impact by enabling constant connectivity, anonymous or pseudonymous contact, and persistent traces that are difficult for victims to manage or erase [2, 32, 45]. Emerging technologies such as Internet of Things (IoT) devices, location tracking, and generative media further expand the ways in which abuse can be enacted and concealed [1, 25, 42, 43]. These developments pose direct challenges to digital well-being and mental health [34, 36, 40] and undermine the UN Sustainable Development goals of gender equality and reduced inequalities [9, 26].

Existing research has documented a wide range of TFA scenarios, including intimate partner surveillance [2, 11], image-based abuse [9, 18, 38, 48], financial sextortion [29, 36], and online harassment [1, 17, 25, 38, 41, 42]. Most studies rely on surveys [2, 9, 16, 17, 19, 29, 45], interviews [1, 6–8, 12, 14, 15, 20, 22, 24, 38, 42], or small scale qualitative analyses [13, 32, 36, 37, 43, 44, 47–49] focused on specific populations or platforms. These approaches provide rich insight into lived experience, but they often lack a systematic way to compare different forms of TFA abuse and the kinds of resources that are supposed to prevent, detect, or respond to them. In particular, there is no widely adopted taxonomy that jointly covers TFA types, preventive measures, detection mechanisms, and support services. This makes it difficult to reason about coverage and gaps in current responses, both in the research literature and in the web resources that people encounter when seeking help. It also limits

Conference'17, Washington, DC, USA

ACM ISBN 978-x-xxxx-xxxx-x/YYYY/MM
https://doi.org/10.1145/nnnnnnn.nnnnnnn

the creation of reusable datasets for vulnerable populations and hinders replicable, data driven analyses of how institutional web content contributes to or mitigates harm.

To address this gap, we first ask how prior work conceptualises the life cycle of TFA, from prevention before abuse occurs to detection while it is ongoing, and subsequently, support after harm has taken place. We then examine how this landscape is reflected in web-based resources provided by institutions, focusing on public and social service websites that people are likely to encounter when they search for information or assistance. Our study is guided by the following research questions:

RQ1: What are the different types of TFA, and which aspects, such as detection, prevention, and support, have been addressed in the literature?

RQ2: What facilities or support services are currently available through the government, non-government organisations (NGOs), and related agencies on the web, and how are these resources framed emotionally and presented in terms of readability and accessibility?

RQ3: What are the existing shortcomings in current responses to TFA, and what strategies can be implemented to strengthen future prevention and support efforts?

To answer these questions, we conduct a structured review of 38 peer-reviewed papers and practitioner reports on TFA and related harms [1, 2, 6–9, 11–17, 19, 20, 22–26, 29, 31, 32, 34, 36–38, 40–49]. From this extensive review, we derive four interconnected taxonomies that capture (1) TFA types, (2) prevention strategies before abuse, (3) detection mechanisms during abuse, and (4) support services after abuse. Together, this TFA taxonomy defines a common set of categories that can be used to (i) benchmark how different web ecosystems cover the TFA life cycle in the resources they offer to victim survivors, (ii) monitor institutional web responses over time by reapplying the taxonomy to new crawls or policy updates, (iii) build labelled datasets for training and evaluating classification or retrieval systems that surface TFA-related resources, and (iv) provide a concrete checklist for designing or auditing public-facing websites and policies. It therefore serves both as an analytic lens for this study and as a reusable scaffold for future, comparable, data-driven work on TFA-related web resources.

As an Australian case study of how this taxonomy can be applied to real-world web infrastructures, we investigate the current state of web-based resources for people affected by TFA by analysing institutional domains registered in Australia. We crawl 306 government, non-government, and relevant commercial domains and collect 52 605 unique web pages that contain content related to domestic and family violence, online safety, or digital abuse. Using a hierarchical zero-shot topic modelling pipeline based on our TFA taxonomy, we perform multi-label classification of each page into abuse types and corresponding prevention, detection, and support categories. Beyond taxonomy-aligned classification, we automatically characterise the dominant emotion and readability of each page using a RoBERTa-based emotion classifier and a suite of readability metrics, which allows us to study not only what information is present but also how it is framed and how accessible it is to different audiences. Here, we use the term "audit" in the sense common to web research, namely a systematic, data-driven assessment of the information exposed through institutional web pages, evaluated against a structured taxonomy of expected content. Our analysis reveals the following:

(1) Web resources are dominated by three abuse types i.e., *Comments Abuse* (30% of the corpus), *Harassment* (26%), and *Sexual Abuse* (14%), which together account for roughly two thirds of all pages. By contrast, *Economic Abuse*, *Privacy Violation*, and *Controlling Behaviours* each appear on fewer than 1% of pages.
(2) In the prevention and detection stages, institutional pages primarily foreground legal and clinical responses. For prevention, *Legal Measures* account for 49% of pages and *Family Safeguarding* for 15%, while *Technology Based Safeguards*, *Public Awareness and Education*, and *Digital Community Networks* together cover less than 1%. For detection, *Clinical Detection* (49%) and *Incidental Discovery* (21%) dominate, whereas *Institutional and Community Reporting* and *Device Detection* are effectively absent.
(3) Support-related content is concentrated in generic digital help and technical safety advice. *Digital Support Infrastructure* accounts for 62% of support pages and *Technology Security Support* for 8%, while *Institutional Support*, *Psychological Support*, *Informal Support Networks*, and *Legal Support* each cover fewer than 1% of pages, with legal support never appearing as a distinct category.
(4) Emotion and readability profiling shows that institutional content is often emotionally neutral but linguistically demanding, and that underrepresented harms tend to be framed with more intense negative affect. Core categories such as *Digital Support Infrastructure*, *Legal Measures*, and *Harassment* are predominantly neutral in tone (around 40% to 50% of pages per category) and are written at reading levels associated with late secondary or early tertiary education. In contrast, rare categories such as *Economic Abuse* and *Privacy Violation* are dominated by fear (up to 90.5% of pages for *Economic Abuse*) and have lower accessibility scores, making them both harder to locate and harder to comprehend.

These findings highlight substantial gaps between the harms documented in the literature and the help that is visible to people who rely on institutional websites for information and support around TFA. They also illustrate how web scale audits grounded in a shared TFA taxonomy can make institutional responses more transparent, enable collaboration between data owners and problem owners, and inform the design of web resources that better promote safety, equity, and social impact for those affected by TFA. The remainder of the paper is organised as follows. Section 2 introduces the TFA taxonomy derived from the literature. Section 3 presents our Australian web case study, including data collection, taxonomy-aligned classification, and emotion and readability assessment. We conclude in Section 4.

2 TFA Taxonomy Creation

In this section, we explain how we derived the TFA taxonomy based on prior work. In line with the lifecycle perspective outlined in Section 1, the taxonomy distinguishes between (1) abuse types, (2) prevention strategies before or between incidents, (3) detection mechanisms while abuse is ongoing, and (4) support measures after

harm has occurred. We later use this shared label space to analyse institutional web content at scale.

2.1 Literature Search

Given the rapid evolution of TFA, we focused on recent work. We queried Google Scholar and major digital libraries using combinations of terms such as "technology facilitated abuse", "tech abuse", "intimate partner surveillance", "image based abuse", and "online harassment", targeting leading venues in security, privacy, and human computer interaction (for example CHI, SOUPS, USENIX Security, IEEE Security & Privacy) and relevant journals. We restricted our corpus to papers published after 2020, with one earlier foundational review [26]. After screening titles and abstracts, we retained 38 papers and practitioner reports that provided empirical data or conceptual frameworks on TFA. Based on the papers, we define four dimensions that mirror the abuse life cycle: (1) abuse types, (2) prevention strategies, (3) detection mechanisms, and (4) support measures. Through iterative coding and constant comparison, we grouped similar concepts into higher-level categories, which form the four taxonomies.

2.2 TFA Types Taxonomy

Building on typologies of digital dating abuse, cyberstalking, image-based abuse, and online sexual harassment [26], we group TFA into six main categories (Figure 1) and refine each with subcategories grounded in prior work:

- **Harassment** captures threatening or repetitive abuse via digital channels, informed by studies of online harassment and workplace digital sexual harassment [19, 26, 41]. Subcategories include direct threats of eviction or physical and sexual violence, technology-mediated harassment via email, messaging, and mobile apps, doxxing or exposure of personal information, and harassment through smart home and VR systems [1, 42].
- **Sexual abuse** covers coercive or non-consensual sexual behaviours facilitated by technology, including image-based sexual abuse, non-consensual pornography, and financially motivated sextortion [28, 34, 36, 38, 48]. Subcategories include recorded sexual assault, grooming, online sexual solicitation, image-based abuse and non-consensual pornography, child sexual exploitation material, and AI-generated sexual content [44].
- **Comments abuse** includes public shaming, hate speech, misinformation, and online humiliation, drawing on studies of digital harassment in workplaces and social platforms [19].
- **Privacy violations** involve unauthorized access, covert surveillance, and exposure of private information [12, 23, 25, 31]. Subcategories include threats to share private or financial material, posting financial information online, unauthorized access to accounts, reading private messages, and covert monitoring of social media [44].
- **Economic abuse** draws on research on technology mediated financial coercion and exclusion [6, 7, 15]. Subcategories include financial extortion and sextortion [28, 36, 47], online scams and fraud, credit abuse or debt manipulation in the victim's name, and reputation attacks that cause economic harm.
- **Controlling behaviours** include location tracking, parental surveillance, digital dating abuse, coercive control, and cyberstalking via spyware and monitoring tools [9, 20, 22, 24, 25, 43–46, 49].

This taxonomy provides the label space for our abuse type classification, allowing us to distinguish, for example, pages focused on sextortion from those focused on parental tracking.

2.3 TFA Prevention Strategies Taxonomy

Prevention work, as depicted in Figure 2 spans legal, social, and technical interventions that aim to reduce the risk of TFA before or between incidents:

- **Legal Measures** include criminalisation of image-based abuse, cyberstalking, and coercive control, civil penalties, and legal literacy programs that inform people about rights and protections [10, 13, 22, 26, 27].
- **Family Safeguarding** covers early warning and safe disclosure mechanisms for children, older adults, disabled people, and other vulnerable groups [22, 41, 42]. Subcategories include observing changes in emotional or digital behaviour and balancing protective monitoring with risks of over-surveillance [44, 49].
- **Community-based Prevention** includes NGO led resource provision and navigation, early intervention consultations, and efforts to shift social norms around harassment, victim blaming, and gender inequality [22, 26, 41, 48].
- **Digital Community Networks** provide prevention-oriented peer support and early warning information through online platforms that share red flags and digital safety practices [22, 41].
- **Public Awareness and Education** include public campaigns, workplace policies and training [19], and school-based curricula on online safety, healthy relationships, consent, and digital ethics [26].
- **Technology-based Safeguards** include anti stalking and tracker detection apps [24, 25], safer access control and notification design for smart devices [43], and financial sector tools to detect abuse related transactions [6, 7].

In our web analysis, these labels indicate whether a page presents TFA only as a problem or also points to concrete preventive measures, and of what kind.

2.4 TFA Detection Mechanisms Taxonomy

The transition from hidden or normalised behaviour to recognised abuse often depends on how TFA is detected. Prior work points to several distinct mechanisms, as presented in Figure 3:

- **Incidental Discovery** covers cases where abuse is uncovered unintentionally, such as the unexpected discovery of trackers, hidden cameras, or monitoring tools, or disclosure of tech abuse during unrelated therapy, legal, or support encounters [42].
- **Clinical Detection** involves in-person professional assessments and digital security audits in which therapists, lawyers,

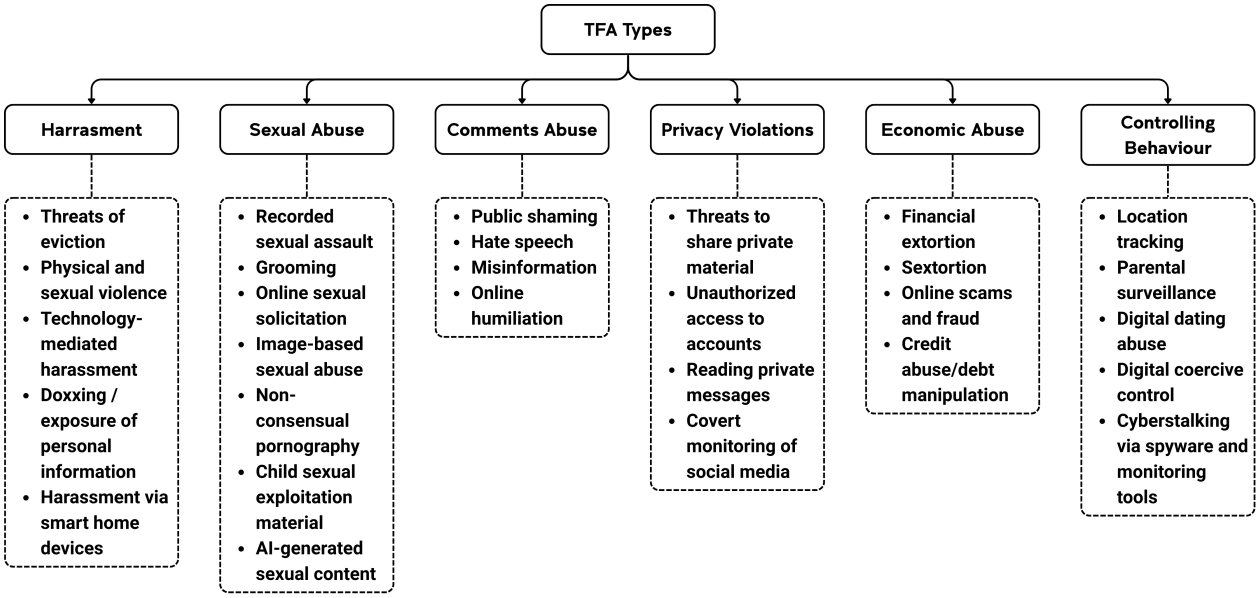

Figure 1: Taxonomy of technology facilitated abuse types.

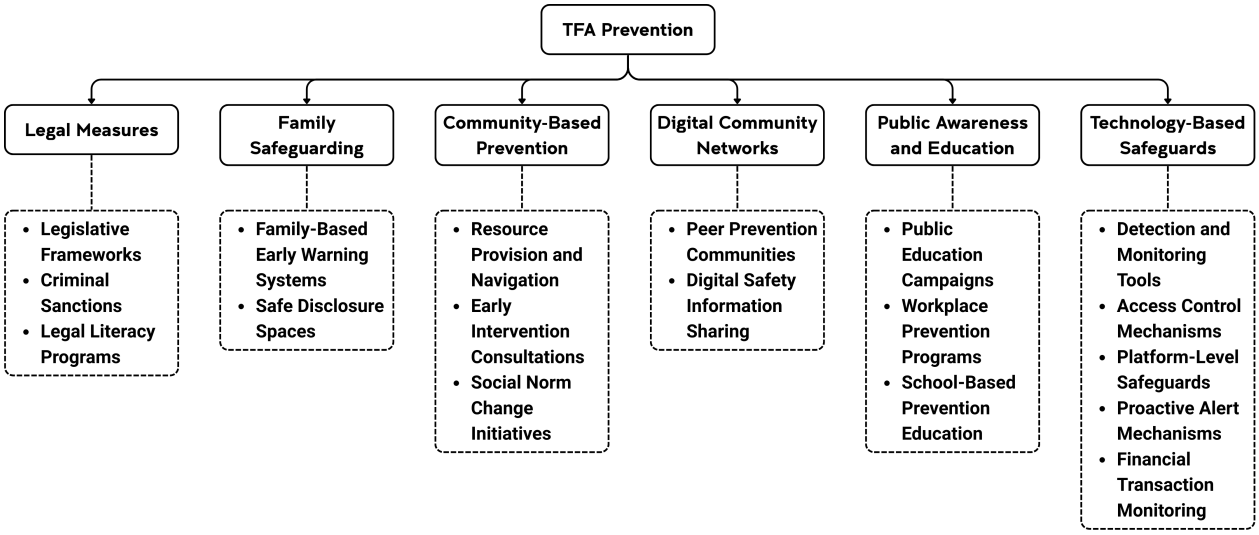

Figure 2: Taxonomy of technology facilitated abuse prevention strategies.

social workers, or security specialists combine survivor narratives with structured device and account checks and recognise patterns of coercive control or surveillance [12, 20, 23].

- **Digital Channel Detection** includes remote security clinics [12], peer forums where survivors recognise patterns in shared narratives [47, 48], and vulnerability research programs that expose abuse vectors in platforms and services [7].
- **Institutional & Community Reporting** covers citizen reporting infrastructures such as online forms and hotlines, community monitoring and moderation, and law enforcement or regulatory investigations that respond to reports of TFA [8, 16, 26, 41, 47].
- **Survey-Based Discovery** reflects the role of anonymous questionnaires and interviews in helping participants identify their experiences as abuse and in documenting patterns of monitoring, threats, and coercion [9, 16, 17, 42].
- **Device Detection** includes manual examination of devices and accounts, automated spyware scans [20], Bluetooth tracker scanning and forensic reconstruction of stalking histories [25, 37], classifier-based detection of suspicious online behaviour [2], and audits that reveal privacy and security flaws that can be abused [7, 11].

Together with the prevention taxonomy, these detection labels let us assess whether institutional pages point towards concrete

ways of identifying TFA, such as device scans or reporting channels, or stay at a purely conceptual level.

2.5 TFA Support Measures Taxonomy

Once abuse is recognised, survivors may seek ongoing support across technical, social, legal, and psychological domains. We present the taxonomy in Figure 4. Prior work describes a mix of formal and informal pathways, which we group into six categories:

- **Digital Support Infrastructure** bundles online support communities [22, 41], remote security services and guidance [2, 12], official reporting portals [26], and curated safety information resources.
- **Technology Security Support** covers specialised help for device security, account protection, and safety configuration, including technology-integrated support centres, customised safety interventions, and guided configuration help for privacy settings and authentication [22, 23].
- **Institutional Support** includes structured survivor assistance programs, domestic and family violence services, and offender intervention programs that combine mediation, behaviour change, and accountability [8, 16].
- **Psychological Support** includes individual counselling and trauma-focused therapy for survivors of sextortion, image-based abuse, and other TFA [28, 47], and integrated mental health care in redress and victim support schemes.
- **Legal Support** spans institutional legal mechanisms such as criminal justice and compensation, civil legal remedies including protection orders and damages claims, and direct legal assistance and advocacy by NGOs [26].
- **Informal Support Networks** reflects assistance from friends, family, and community organisations, which often act as first responders and intermediaries when survivors seek help [17, 22, 41].

These four taxonomies operationalise the TFA lifecycle introduced in Section 1 along four dimensions: what kinds of abuse occur, how they might be prevented, how they are detected, and what support is offered afterwards. In the remainder of the paper, we use this shared label space to classify Australian institutional websites to quantify where online resources align with, or fall short of, the TFA prevention, detection, and support needs.

3 Case Study of Australian Domains

Australia offers a uniquely important case study for TFA because the country is simultaneously experiencing some of the highest recorded rates of domestic, family, and sexual violence among OECD nations, and is also home to ambitious national initiatives aimed at prevention, digital safety, and survivor support[1]. Recent surveys show that 1 in 4 Australian women and 1 in 8 men have experienced intimate-partner violence, and an estimated 65-70% of domestic-violence survivors report technology-enabled harassment, monitoring, or threats, placing TFA at the centre of national policy concern [5, 33, 35]. The Australian Government has invested more than $2.3 billion under the National Plan to End Violence Against Women and Children (2022-2032), including targeted programs addressing online harms, safety by design, and tech-abuse prevention in partnership with eSafety, state governments, and frontline services [3, 4]. Compared to many countries, Australia also maintains a strong institutional infrastructure, some being the eSafety Commissioner, national domestic-violence hotlines, and state-level women's safety initiatives, making it an ideal environment to evaluate how public institutions communicate risks and support pathways around TFA.

[1]https://www.esafety.gov.au/women/reduce-technology-facilitated-abuse; Accessed on 28 November 2025

3.1 Data Collection

Domain selection. We first identified Australian web domains likely to contain TFA-related content using advanced Google search operators (for example, `site:.au` combined with 32 TFA-specific keywords derived from our literature review). This yielded 2,212 candidate domains referencing phenomena such as "image-based abuse", "online harassment", and "technology-facilitated coercive control". We manually screened all domains and retained 306 that provided substantive information or support related to domestic and family violence, online safety, or digital abuse. General media sites (e.g., `9news.com.au`), where TFA keywords occurred only sporadically in isolated articles, were excluded. By contrast, domains whose primary purpose is related to child protection, safety, or advocacy (such as `actparents.org.au`) were retained.

Crawling and content extraction. For each domain, we deployed a custom web crawler based on depth-first search (DFS) with a maximum traversal depth of four. Crawling began from a domain-specific entry URL and followed internal links either across the full domain (for small and medium sites) or within chosen subdirectories (for large sites). Newly discovered internal URLs were added to a stack until the depth limit was reached. Unsupported MIME types, such as spreadsheets, compressed archives, and multimedia, were discarded. HTML pages were rendered using Playwright with a headless Chromium backend to ensure complete DOM extraction, and the resulting HTML source was stored in our database. Extremely large domains that would require more than one hour of crawling were handled manually by identifying TFA-relevant entry points and restricting traversal to URLs sharing those prefixes.

Preprocessing. The raw crawl produced 56,672 URLs across 306 domains. We applied a multi-stage preprocessing pipeline to extract visible textual content, removing boilerplate such as navigation menus, scripts, and style blocks. We further filtered pages with empty or near-empty text, pages below a minimum length threshold, and pages failing an English-language check. The final dataset comprises 52,605 cleaned pages (Table 1).

3.2 Taxonomy-Aligned Classification

To align the corpus with the four taxonomy dimensions introduced in Section 2, we perform hierarchical multi-label text classification. Each cleaned page is mapped to one or more primary categories in each taxonomy and, where supported by sufficient evidence, to corresponding subcategories. All label predictions are constrained strictly to the predefined taxonomy structures.

Primary category classification. For each taxonomy (abuse, prevention, detection, support), we classify web pages at the level of

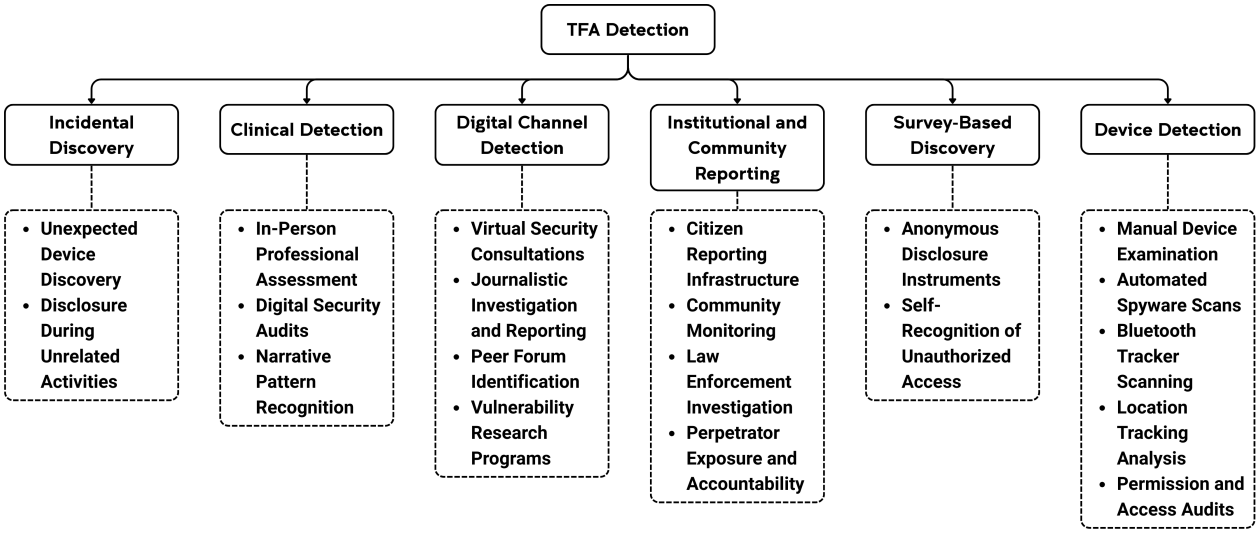

Figure 3: Taxonomy of technology-facilitated abuse detection mechanisms.

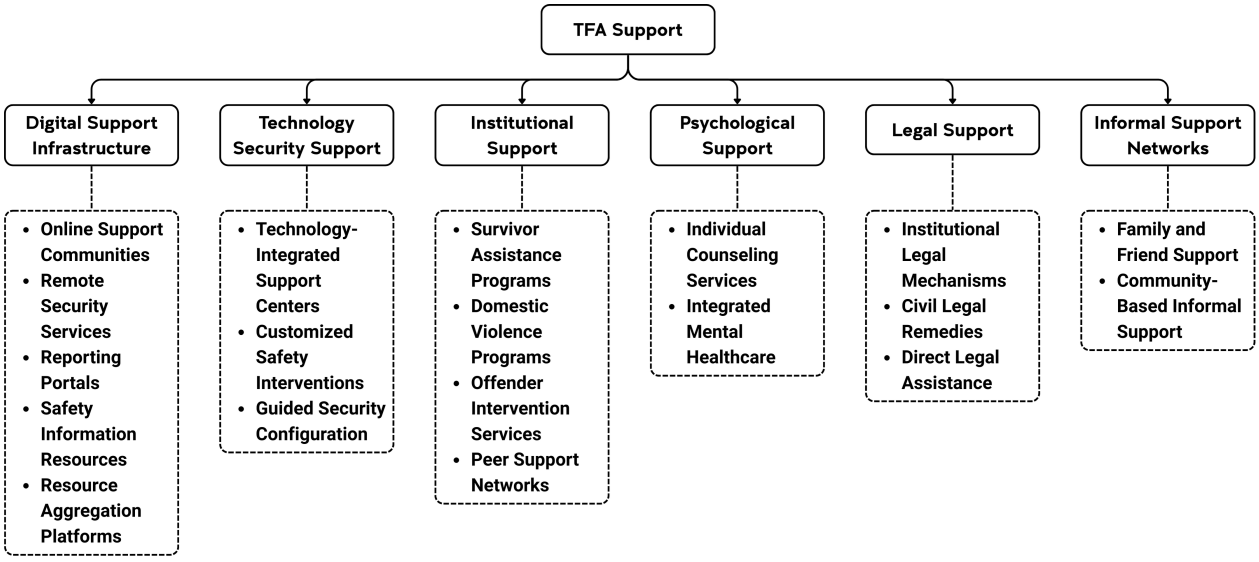

Figure 4: Taxonomy of technology-facilitated abuse support measures.

primary categories. We embed each web page using all-MiniLM-L6-v2[2], a SentenceTransformer model [39], and apply zero-shot BERTopic [21] with the primary taxonomy categories as candidate labels. The model uses (i) all-MiniLM-L6-v2 for embeddings, (ii) deberta-v3-large-zeroshot-v2.0[3] as a zero-shot similarity model, and (iii) a similarity threshold of 0.5. Categories meeting or exceeding this threshold are retained, yielding a multi-label assignment.

Subcategory classification. For each primary category, we select all web pages assigned that label and apply a second zero-shot BERTopic model restricted to the subcategories of that primary category. This produces a refined, category-specific multi-label assignment. To avoid unstable models on small subsets, subcategory classification is performed only when a primary category contains at least 15 web pages; otherwise the taxonomy assignment remains at the primary level. A similarity threshold of 0.5 is again applied.

3.3 Emotion and Readability Assessment

To understand not only *what* institutions say about TFA but also *how* they communicate it, we analyse each web page along two complementary axes: affective framing and textual accessibility. Emotion profiles indicate whether institutional narratives emphasise fear, neutrality, reassurance, or other stances, while readability

[2]https://huggingface.co/sentence-transformers/all-MiniLM-L6-v2
[3]https://huggingface.co/MoritzLaurer/deberta-v3-large-zeroshot-v2.0

Top 10 Domains	μ_{word}	Count
southsafe.org.au	368.8	3297
fcfcoa.gov.au	511.9	2129
ndiscommission.gov.au	264.6	1864
legalaid.wa.gov.au	314.8	1717
gcyp.sa.gov.au	269.5	1589
professionals.childhood.org.au	455.2	1428
lwb.org.au	532.1	1256
criminal-lawyers.com.au	668.9	1207
legalaid.vic.gov.au	610.1	1193
headtohealth.gov.au	150.3	1191
Total	**397.8**	**52605**

Table 1: Average number of words per page μ_{word} and total page counts for the ten largest domains in the corpus, together with aggregate statistics for the full dataset.

metrics capture how easy it is for survivors, practitioners, and the general public to engage with the information.

Emotion classification. We apply a RoBERTa-based [30] English emotion classifier[4] that outputs seven mutually exclusive emotions: anger, disgust, fear, joy, neutral, sadness, and surprise. For each web page we retain the dominant emotion (highest-scoring class). At the taxonomy level, we compute the proportion of web pages whose dominant emotion corresponds to each label, yielding the emotion distributions.

Readability and accessibility. We compute readability indicators using `textstat`[5], including Flesch Reading Ease (higher indicates easier text) and the Automated Readability Index (higher indicates more complex text). We also define a composite accessibility score (0-100) that penalises long sentences, long paragraphs, and high grade-level scores. Category-level readability scores are obtained by averaging over all web pages assigned to each taxonomy category.

3.4 Analysis of Taxonomy Coverage, Emotion, and Accessibility

Table 2 summarises how the 52,605 web pages in our corpus are distributed across the four taxonomy dimensions, and how these categories differ in affective tone and linguistic accessibility. Below, we interpret these results in relation to our three research questions.

3.4.1 RQ1: Coverage of TFA types, detection, prevention, and support. The taxonomy-aligned classification operationalises the literature-derived conceptual model of TFA (Section 2) at scale. Across abuse types, institutional web content overwhelmingly foregrounds *Comments Abuse* (30%) and *Harassment* (26%). *Sexual Abuse* appears in 14% of the corpus, but other categories identified in the TFA literature are underrepresented in the Australian domains. These include *Privacy Violation*, *Economic Abuse*, and *Controlling Behaviours*, each appearing in fewer than 1% of pages. Their emotion profiles further signal their marginalisation: pages on *Privacy Violation* are dominated by *Fear* (38.1%) and *Anger* (33.6%), while *Economic Abuse* is overwhelmingly classified as *Fear* (90.5%). A similar pattern arises for detection, prevention, and support. In detection, institutional content is dominated by *Clinical Detection* (49%) and *Incidental Discovery* (21%), whereas categories representing systematic detection infrastructures such as *Institutional and Community Reporting* and *Device Detection* do not appear in the corpus at all. Within prevention, nearly half of all relevant pages concern *Legal Measures* (49%), followed by *Family Safeguarding* (15%). As shown in Table 3 (Appendix A), the most common subcategories within these types reinforce this focus on visible, public-facing harms. For instance, the dominant *Comments Abuse* subcategory is *Public Shaming*, *Harassment* is often instantiated as *Threats of Eviction*, and *Sexual Abuse* is frequently framed as *Recorded Sexual Assault*. In contrast, there are far fewer pages that describe covert surveillance, financial coercion, or long-term controlling behaviours in detail, despite their prominence in the research taxonomy. The most frequent detection subcategories, *In Person Professional Assessment* and *Unexpected Device Discovery*, show that TFA is often framed as something that comes to light during face-to-face consultations or by chance, rather than through dedicated tools or reporting systems. Prevention measures are instantiated as *Criminal Sanctions* and *Family-Based Early Detection*. Categories emphasised in research as forward-looking and technology-centric, such as *Technology Based Safeguards* and *Public Awareness and Education*, together account for less than 1% of pages. Support content is similarly skewed: *Digital Support Infrastructure* accounts for 62% of support-related pages, and its most common subcategory, *Online Support Communities*, appears on 25,912 (out of 52,605) pages. By comparison, *Technology Security Support*, *Institutional Support*, and *Psychological Support* have far fewer pages and smaller subcategory counts.

3.4.2 RQ2: Web-facing facilities and support services. For survivors, practitioners, or the public accessing institutional websites, the most visible and accessible facilities are those tied to *Digital Support Infrastructure* (62%) and *Technology Security Support* (8%). These categories also display largely neutral emotion profiles (45.6% and 40.4% neutral respectively) and mid-range accessibility scores (59.70 and 58.13), which is consistent with informational self-help content aimed at broad audiences. The distribution of support-related categories indicates that institutional websites overwhelmingly prioritise informational guidance over actionable service pathways. Almost two-thirds of all support pages fall under *Digital Support Infrastructure*, whereas categories directly associated with service access such as *Institutional Support*, *Psychological Support*, *Informal Support Networks*, and *Legal Support* collectively account for under 2% of pages, with *Legal Support* entirely absent. As shown in Table 4 (Appendix B), sites associated with *Digital Support Infrastructure*, such as `southsafe.org.au`, `fcfcoa.gov.au`, and `ndiscommission.gov.au`, primarily offer static information hubs, downloadable resources, and broad safety guidance. Content mapped to *Technology Security Support* on domains such as `gcyp.sa.gov.au` or `legalaid.vic.gov.au` focuses on high level digital safety advice, device configuration, and account protection, but often does not provide direct mechanisms for live digital security assistance. By contrast, *Institutional Support* and *Psychological Support* tend to appear as brief descriptions of programs or counselling services that require additional navigation or offline steps to access. Mentions of *Informal Network Support* are particularly sparse, appearing only on a small number of pages.

[4] https://huggingface.co/j-hartmann/emotion-english-distilroberta-base
[5] https://docs.textstat.org/

Category	Corpus (%)	Emotion (%)							Readability		
		Neutral	Joy	Fear	Sadness	Anger	Surprise	Disgust	Flesch (↑)	ARI (↓)	Access. (↑)
TFA Types											
Harassment	26	**41.5**	21.4	13.4	12.2	6.9	3.9	0.7	25.07	20.27	59.16
Sexual Abuse	14	**40.6**	19.4	11.7	14.4	9.2	3.8	0.9	30.49	18.01	59.18
Comments Abuse	30	**48.3**	18.6	11.3	11.5	5.4	4.3	0.6	24.00	21.48	59.46
Privacy Violation	<1	17.2	2.8	**38.1**	6.3	33.6	0.4	1.8	31.58	16.56	42.50
Economic Abuse	<1	0.3	0.2	**90.5**	0.3	8.6	0.1	0.1	31.10	**11.70**	65.00
Controlling Behaviours	<1	**81.5**	3.5	4.0	2.1	4.2	2.2	2.5	**31.95**	14.97	**69.62**
TFA Prevention											
Legal Measures	49	**44.6**	18.1	11.4	13.6	7.6	4.1	0.7	27.08	19.92	59.55
Family Safeguarding	15	**47.0**	18.9	12.5	11.2	5.7	3.9	0.8	19.35	22.41	57.57
Community-Based Prevention	6	**41.5**	24.6	13.3	12.0	4.3	3.9	0.5	26.22	20.64	60.46
Digital Community Networks	0	–	–	–	–	–	–	–	–	–	–
Public Awareness and Education	<1	**53.9**	11.9	25.8	1.8	3.9	2.5	0.3	-8.68	29.03	42.06
Technology-Based Safeguards	<1	23.0	**50.5**	2.9	2.7	17.7	3.1	0.2	**38.98**	**13.87**	**75.00**
TFA Detection											
Clinical Detection	49	**51.3**	20.7	8.9	11.8	4.0	2.8	0.6	13.07	24.18	58.84
Incidental Discovery	21	**45.0**	19.3	12.4	12.0	6.6	4.1	0.7	25.31	20.61	59.21
Digital Channel Detection	<1	31.5	2.2	**51.4**	6.7	1.5	6.6	0.2	**38.90**	15.29	53.46
Survey-Based Discovery	<1	9.2	1.0	0.6	**83.1**	4.9	0.8	0.4	29.41	**13.72**	**65.00**
Institutional & Community Reporting	0	–	–	–	–	–	–	–	–	–	–
Device Detection	0	–	–	–	–	–	–	–	–	–	–
TFA Support											
Digital Support Infrastructure	62	**45.6**	19.2	11.5	12.5	6.4	4.2	0.6	24.04	21.07	59.70
Technology Security Support	8	**40.4**	13.8	14.4	16.3	10.8	3.3	0.9	34.38	16.38	58.13
Institutional Support	<1	**39.7**	24.7	15.9	11.7	4.7	2.8	0.7	33.19	17.23	58.21
Psychological Support	<1	**43.2**	6.6	32.1	9.3	6.4	2.0	0.5	28.69	16.38	50.73
Legal Support	0	–	–	–	–	–	–	–	–	–	–
Informal Support Networks	<1	**81.2**	11.1	1.4	2.0	1.6	2.5	0.2	**55.48**	**14.32**	**66.50**

Table 2: Summary of TFA web content across taxonomy dimensions, showing category coverage in the corpus, distributions of dominant predicted emotions, and average readability scores. Higher Flesch and accessibility values indicate easier text, while higher ARI reflects more complex text; "–" denotes categories with no classified documents.

3.4.3 RQ3: Gaps and opportunities for strengthening responses. The combination of coverage, emotion, readability, and subcategory patterns reveals systematic gaps that point to concrete avenues for strengthening TFA responses. First, there is a pronounced gap between the harms emphasised in the literature and those visible online. Categories such as *Privacy Violation* and *Economic Abuse* are nearly absent (less than 1%) and are emotionally dominated by *Fear* (38.1% and 90.5% respectively). Their low volume and high emotional intensity risk making them both difficult to locate and cognitively burdensome to process. Expanding coverage and presenting clearer, stepwise guidance in these areas would better align institutional communication with empirical TFA research. Second, prevention and detection content remains largely reactive rather than proactive. The absence of *Technology Based Safeguards*, *Institutional and Community Reporting*, and *Device Detection* suggests that institutional sites undercommunicate actionable, technology-driven countermeasures, even though these feature prominently in technical and policy literatures on anti stalking, tracker detection, and safety by design. Incorporating descriptions of detection tools, reporting workflows, and platform-level protections could materially strengthen web-facing prevention and detection. Third, readability metrics indicate that many categories fall within late secondary or early tertiary reading levels. Automated Readability Index (ARI) values for central categories often lie between 18 and 22, with accessibility scores in the range of 50 to 60. For instance, the *Harassment* category reflects an ARI of 20.27 and an accessibility score of 59.16, while *Comments Abuse* shows ARI 21.48 with a score of 59.46. According to recent data from the Australian Bureau of Statistics[6], approximately 73% of Australians aged 25 to 34 hold a Certificate III qualification or higher, meaning that nearly one in four adults may have lower formal education. Content written at tertiary reading levels may therefore pose undue difficulty for many at risk users. Notably, underrepresented categories such as *Economic Abuse* and *Privacy Violation*, despite their emotional intensity, receive less than 1% of pages and often use complex language and dense structure. By contrast, *Informal Support Networks*, although it occupies less than 1% of the corpus, achieves a higher Flesch Reading Ease score (55.48) and accessibility score (66.50), illustrating that more accessible content is possible but rare. Co design with community partners may therefore help institutions produce guidance that is both clearer and more supportive [16, 22].

Takeaway: *Our analysis shows that Australian institutional web content is strongest where it provides legal framing, high-level information hubs, and digital safety guidance, but weaker in conveying covert harms, technological prevention, systematic detection, and multidimensional support pathways.*

4 Conclusion

This paper proposed a unified taxonomy of TFA, synthesising peer-reviewed studies into four dimensions (types, prevention, detection, support). The taxonomy was operationalised through a large-scale

[6]https://www.abs.gov.au/statistics/people/education

audit of 306 Australian institutional domains and 52,605 web pages using hierarchical zero-shot classification, emotion analysis, and readability profiling. Our results show that institutional content concentrates on harassment, comments abuse, and sexual abuse, while covert, privacy related, and economic abuse together account for fewer than 1% of pages; that prevention and detection information is heavily skewed toward legal framing and incidental discovery, with proactive, technology based safeguards and reporting infrastructures rarely described; and that support is dominated by digital information hubs, with comparatively little web visible guidance into counselling, legal aid, or community based services, often expressed at late secondary or tertiary reading levels. Future work should apply this audit framework to other jurisdictions, examine how these informational gaps shape survivors' help-seeking and decision-making, and build taxonomy-aligned tools that surface clearer, more accessible, and actionable support pathways.

References

[1] SB Abhinaya, Aafaq Sabir, and Anupam Das. 2024. Enabling Developers, Protecting Users: Investigating Harassment and Safety in {VR}. In *33rd USENIX Security Symposium (USENIX Security 24)*. 6561–6578.

[2] Majed Almansoori, Mazharul Islam, Saptarshi Ghosh, Mainack Mondal, and Rahul Chatterjee. 2024. The Web of Abuse: A Comprehensive Analysis of Online Resource in the Context of Technology-Enabled Intimate Partner Surveillance. In *2024 IEEE 9th European Symposium on Security and Privacy (EuroS&P)*. 773–789. doi:10.1109/EuroSP60621.2024.00048

[3] Australian Government Department of Social Services. 2022. National Plan to End Violence Against Women and Children 2022–2032. https://www.dss.gov.au/system/files/resources/national-plan-end-violence-against-women-and-children-2022-2032.pdf. Accessed: 2025-02-25.

[4] Australian Government, Department of the Prime Minister and Cabinet. 2024. Working to Keep Women Safe. https://ministers.pmc.gov.au/gallagher/2024/working-keep-women-safe. Accessed: 2025-02-25.

[5] Australia's National Research Organisation for Women's Safety (ANROWS). 2022. Technology-facilitated abuse: National survey of Australian adults' experiences. https://www.anrows.org.au/publication/technology-facilitated-abuse-national-survey-of-australian-adults-experiences/. Accessed: 2025-02-25.

[6] Rosanna Bellini. 2023. Paying the price: When intimate partners use technology for financial harm. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–17.

[7] R Bellini, K Lee, MA Brown, J Shaffer, R Bhalerao, and T Ristenpart. 2023. The Digital-Safety Risks of Financial Technologies for Survivors of Intimate Partner Violence. USENIX Security Symposium.

[8] Rosanna Frances Bellini. 2024. Abusive partner perspectives on technology abuse: Implications for community-based violence prevention. *Proceedings of the ACM on Human-Computer Interaction* 8, CSCW1 (2024), 1–25.

[9] Cynthia Brown, Lena Sanci, and Kelsey Hegarty. 2021. Technology-facilitated abuse in relationships: Victimisation patterns and impact in young people. *Computers in Human Behavior* 124 (2021), 106897.

[10] California Legislature. 2024. *New California law requires parents to save money earned by child influencers.* https://nypost.com/2024/09/27/us-news/new-california-law-requires-parents-to-save-money-earned-by-child-influencers/ Requires parents to deposit at least 15% of minors' earnings into a trust account until age 18, extending the Coogan Law to social media influencers.

[11] Rose Ceccio, Sophie Stephenson, Varun Chadha, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Sneaky spy devices and defective detectors: the ecosystem of intimate partner surveillance with covert devices. In *32nd USENIX Security Symposium (USENIX Security 23)*. 123–140.

[12] Janet X Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin A Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell. 2022. Trauma-informed computing: Towards safer technology experiences for all. In *Proceedings of the 2022 CHI conference on human factors in computing systems*. 1–20.

[13] Mahfuzulhoq Chowdhury and Jaowad Hassan Noor. 2024. Safe-Guard: A Smartphone Application with Child Abuse Detection, Doctor Selection, Legal Aid, and Child Abuse Case Reporting Help Assistance. In *2024 IEEE International Conference on Contemporary Computing and Communications (InC4)*, Vol. 1. IEEE, 1–6.

[14] Kathryn D Coduto and Allison McDonald. 2024. "Delete it and Move On": Digital Management of Shared Sexual Content after a Breakup. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (Honolulu, HI, USA) *(CHI '24)*. Association for Computing Machinery, New York, NY, USA, Article 918, 16 pages. doi:10.1145/3613904.3642722

[15] Andrew C Dwyer, Lizzie Coles-Kemp, Clara Crivellaro, and Claude PR Heath. 2025. Friend or Foe? Navigating and Re-configuring" Snipers' Alley". *arXiv preprint arXiv:2503.16992* (2025).

[16] Asher Flynn, Anastasia Powell, and Sophie Hindes. 2021. Technology-facilitated abuse: A survey of support services stakeholders. (2021).

[17] Asher Flynn, Anastasia Powell, and Sophie Hindes. 2022. *Technology-facilitated abuse: National survey of Australian adults' experiences.* Australia's National Research Organisation for Women's Safety (ANROWS).

[18] Asher Flynn, Anastasia Powell, Adrian J Scott, and Elena Cama. 2022. Deepfakes and digitally altered imagery abuse: A cross-country exploration of an emerging form of image-based sexual abuse. *The British Journal of Criminology* 62, 6 (2022), 1341–1358.

[19] ASHER FLYNN, ANASTASIA POWELL, and LISA WHEILDON. 2024. Workplace technology-facilitated sexual harassment. (2024).

[20] Diana Freed, Sam Havron, Emily Tseng, Andrea Gallardo, Rahul Chatterjee, Thomas Ristenpart, and Nicola Dell. 2019. " Is My Phone Hacked?" Analyzing Clinical Computer Security Interventions With Survivors of Intimate Partner Violence. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–24.

[21] Maarten Grootendorst. 2022. BERTopic: Neural topic modeling with a class-based TF-IDF procedure. arXiv:2203.05794 [cs.CL] https://arxiv.org/abs/2203.05794

[22] Naman Gupta, Kate Walsh, Sanchari Das, and Rahul Chatterjee. 2024. " I really just leaned on my community for support": Barriers, Challenges, and Coping Mechanisms Used by Survivors of {Technology-Facilitated} Abuse to Seek Social Support. In *33rd USENIX Security Symposium (USENIX Security 24)*. 4981–4998.

[23] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*. 105–122.

[24] Alexander Heinrich, Niklas Bittner, and Matthias Hollick. 2022. AirGuard-protecting android users from stalking attacks by apple find my devices. In *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 26–38.

[25] Alexander Heinrich, Leon Würsching, and Matthias Hollick. 2024. Please Unstalk Me: Understanding Stalking with Bluetooth Trackers and Democratizing Anti-Stalking Protection. *Proceedings on Privacy Enhancing Technologies* (2024).

[26] Nicola Henry, Asher Flynn, and Anastasia Powell. 2020. Technology-facilitated domestic and sexual violence: A review. *Violence against women* 26, 15-16 (2020), 1828–1854.

[27] Illinois General Assembly. 2023. *Illinois amends Child Labor Law to protect children featured in family vlogs.* https://www.americanbar.org/content/dam/aba/publications/Jurimetrics/spring-2024/family-vlogging-and-child-harm-a-need-for-nationwide-protection.pdf Mandates that parents put aside a percentage of earnings from for-profit family vlogs into a trust fund for the child, effective July 2024.

[28] Roberta Liggett O'Malley and Katelyn Smith. 2024. Suicidal Ideation Among Male Victim-Survivors of Financial Sextortion. *Victims & Offenders* 20, 7 (July 2024), 1285–1306. doi:10.1080/15564886.2024.2379818

[29] Roberta Liggett O'Malley and Katelyn Smith. 2025. Suicidal Ideation Among Male Victim-Survivors of Financial Sextortion. *Victims & Offenders* 20, 7 (2025), 1285–1306.

[30] Yinhan Liu, Myle Ott, Naman Goyal, Jingfei Du, Mandar Joshi, Danqi Chen, Omer Levy, Mike Lewis, Luke Zettlemoyer, and Veselin Stoyanov. 2019. RoBERTa: A Robustly Optimized BERT Pretraining Approach. arXiv:1907.11692 [cs.CL] https://arxiv.org/abs/1907.11692

[31] Philippe Mangeard, Xiufen Yu, Mohammad Mannan, and Amr Youssef. 2023. No Place to Hide: Privacy Exposure in Anti-stalkerware Apps and Support Websites. In *Nordic Conference on Secure IT Systems*. Springer, 18–36.

[32] Dana McKay and Charlynn Miller. 2021. Standing in the way of control: A call to action to prevent abuse through better design of smart technologies. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*. 1–14.

[33] NSW Bureau of Crime Statistics and Research. 2024. Domestic violence statistics. https://bocsar.nsw.gov.au/topic-areas/domestic-violence.html. Accessed: 2025-02-25.

[34] Borke Obada-Obieh, Yue Huang, Lucrezia Spagnolo, and Konstantin Beznosov. 2022. Sok: The dual nature of technology in sexual abuse. In *2022 IEEE Symposium on Security and Privacy (S&P)*. IEEE, 2320–2343.

[35] Australian Institute of Health and Welfare. 2023. Intimate partner violence. https://www.aihw.gov.au/family-domestic-and-sexual-violence/types-of-violence/intimate-partner-violence. Accessed: 2025-02-25.

[36] Roberta Liggett O'Malley. 2023. Short-term and long-term impacts of financial sextortion on victim's mental well-being. *Journal of interpersonal violence* 38, 13-14 (2023), 8563–8592.

[37] Lauren R Pace, LaSean A Salmon, Christopher J Bowen, Ibrahim Baggili, and Golden G Richard III. 2023. Every step you take, I'll be tracking you: Forensic analysis of the tile tracker application. *Forensic science international: digital*

investigation 45 (2023), 301559.
[38] Lucy Qin, Vaughn Hamilton, Sharon Wang, Yigit Aydinalp, Marin Scarlett, and Elissa M Redmiles. 2024. " Did They {F*** ing} Consent to That?": Safer Digital Intimacy via Proactive Protection Against {Image-Based} Sexual Abuse. In *33rd USENIX Security Symposium (USENIX Security 24)*. 55–72.
[39] Nils Reimers and Iryna Gurevych. 2019. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. In *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics. https://arxiv.org/abs/1908.10084
[40] Carol F Scott, Gabriela Marcu, Riana Elyse Anderson, Mark W Newman, and Sarita Schoenebeck. 2023. Trauma-informed social media: Towards solutions for reducing and healing online harm. In *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*. 1–20.
[41] Md Mamunur Rashid Sheikh and Michaela M Rogers. 2024. Technology-facilitated sexual violence and abuse in low and middle-income countries: A scoping review. *Trauma, Violence, & Abuse* 25, 2 (2024), 1614–1629.
[42] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, and Rahul Chatterjee. 2023. " It's the Equivalent of Feeling Like You're in {Jail"}: Lessons from Firsthand and Secondhand Accounts of {IoT-Enabled} Intimate Partner Abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*. 105–122.
[43] Sophie Stephenson, Majed Almansoori, Pardis Emami-Naeini, Danny Yuxing Huang, and Rahul Chatterjee. 2023. Abuse Vectors: A Framework for Conceptualizing {IoT-Enabled} Interpersonal Abuse. In *32nd USENIX Security Symposium (USENIX Security 23)*. 69–86.
[44] Sophie Stephenson, Christopher Nathaniel Page, Miranda Wei, Apu Kapadia, and Franziska Roesner. 2024. Sharenting on TikTok: Exploring parental sharing behaviors and the discourse around children's online privacy. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems*. 1–17.
[45] Kieron Ivy Turk and Alice Hutchings. 2024. Stop Following Me! Evaluating the Malicious Uses of Personal Item Tracking Devices and Their Anti-Stalking Features. In *Proceedings of the 2024 European Symposium on Usable Security*. 277–289.
[46] Kieron Ivy Turk, Alice Hutchings, and Alastair R Beresford. 2023. Can't Keep Them Away: The Failures of Anti-stalking Protocols in Personal Item Tracking Devices. In *Cambridge International Workshop on Security Protocols*. Springer, 78–88.
[47] Fangzhou Wang. 2025. Breaking the silence: Examining process of cyber sextortion and victims' coping strategies. *International Review of Victimology* 31, 1 (2025), 91–116.
[48] Miranda Wei, Sunny Consolvo, Patrick Gage Kelley, Tadayoshi Kohno, Tara Matthews, Sarah Meiklejohn, Franziska Roesner, Renee Shelby, Kurt Thomas, and Rebecca Umbach. 2024. Understanding {Help-Seeking} and {Help-Giving} on Social Media for {Image-Based} Sexual Abuse. In *33rd USENIX Security Symposium (USENIX Security 24)*. 4391–4408.
[49] Miranda Wei, Eric Zeng, Tadayoshi Kohno, and Franziska Roesner. 2022. {Anti-Privacy} and {Anti-Security} Advice on {TikTok}: Case Studies of {Technology-Enabled} Surveillance and Control in Intimate Partner and {Parent-Child} Relationships. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*. 447–462.

A Top Co-occurring Subcategories Across the TFA Taxonomies

Table 3 reports the most frequent subcategories for each primary taxonomy dimension. For TFA types, high counts for *Public Shaming*, *Threats of Eviction*, and *Recorded Sexual Assault* indicate that institutional content largely focuses on overt, visible harms. In the prevention and detection taxonomies, subcategories such as *Criminal Sanctions*, *Family-Based Early Detection*, and *In-Person Professional Assessment* show that responses are commonly framed through legal and clinical interventions rather than technical safeguards or community-level mechanisms. For support, the prominence of *Online Support Communities* relative to categories such as *Security Clinics* or *Survivors Assistance Program* describes the central role of general digital information hubs compared to more intensive, programmatic services.

Category	Subcategory	Count
TFA Types		
Comments Abuse	Public Shaming	11093
Harassment	Threats of Eviction	10297
Sexual Abuse	Recorded Sexual Assault	4310
TFA Prevention		
Legal Support	Criminal Sanctions	21344
Family Safeguarding	Family-Based Early Detection	7200
Community-Based Prevention	Resource Provision and Navigation	3433
TFA Detection		
Clinical Detection	In-Person Professional Assessment	21019
Incidental Discovery	Unexpected Device Discovery	10411
Digital Channel Detection	Virtual Security Consultations	84
TFA Support		
Digital Support Infrastructure	Online Support Communities	25912
Technology Security Support	Security Clinics	3917
Institutional Support	Survivors Assistance Program	334

Table 3: Top co-occurring category pairs for each TFA taxonomy.

B Example Domains Providing TFA Support Services

Table 4 lists example Australian domains associated with each support category, as identified by the subcategory classification. Sites mapped to *Digital Support Infrastructure* are typically information portals and resource hubs, while those associated with *Technology Security Support* tend to provide device and account safety guidance. Domains linked to *Institutional Support*, *Psychological Support*, and *Informal Network Support* are fewer and usually describe programs or referral options at a high level, reflecting the limited visibility of counselling, legal aid, and community-based support within the broader corpus.

Support Category	Example Domains
Digital Support Infrastructure	southsafe.org.au; fcfcoa.gov.au; ndiscommission.gov.au
Technology Security Support	southsafe.org.au; gcyp.sa.gov.au; legalaid.vic.gov.au
Institutional Support	lwb.org.au; legalaid.vic.gov.au; nationallegalaid.org
Psychological Support	legalaid.wa.gov.au; headtohealth.gov.au; medicarementalhealth.gov.au
Legal Support	legalaid.wa.gov.au; legalaid.vic.gov.au; nationallegalaid.org
Informal Network Support	southsafe.org.au; headtohealth.gov.au

Table 4: Example Australian domains that provide different types of Technology-Facilitated Abuse (TFA) support, showing which organisations offer which classes of assistance.