November 2026

Safety by Design guide to preventing coercive control facilitated by technology

An addendum to ‘Technology, gendered violence and Safety by Design’



Australian Government

eSafety Commissioner

eSafety.gov.au

Contents

What is coercive control? **3**
- **Who are the perpetrators?** 3
- **Attitudes that normalise coercive control** 4
- **Who does it affect?** 5
- **What are the impacts?** 7

How is technology used as part of coercive control? **8**
- **Potential signals of coercive control** 11
- **Evolving tactics** 12

Applications of Safety by Design across sectors **15**
- **Considerations with implementation** 16

Practical measures to address coercive control **18**
- **Service provider responsibility** 19
- **User empowerment and autonomy** 23
- **Transparency and accountability** 27
- **Responding to technology-facilitated abuse: eSafety's Technology-Facilitated Abuse Support Service** 30

Conclusion **32**

Content warning: This chapter discusses technology-facilitated coercive control and abuse. Please take care when reading and consider whether this guide is right for you at this time.

Overview

Coercive control is an escalating safety risk for the technology industry, and active steps should be taken to understand and mitigate these risks at the design phase. Increasingly, abusers exploit digital platforms, services and connected devices to monitor, isolate, intimidate and control others. Addressing this harm is a central priority of Australia's National Plan to End Violence against Women and Children 2022–2032, which calls on industry to play a proactive role. In particular, the plan's prevention domain highlights the need to harness technology responsibly by embedding Safety by Design principles to help prevent abuse before it occurs.[1]

This chapter complements eSafety's **industry guide** for addressing technology-facilitated gender-based violence through Safety by Design, published in September 2024. It focuses on **technology-facilitated coercive control** and gives companies practical guidance to help prevent their products and services from being weaponised for abuse. It includes trends, signals, case studies and applications of technical interventions and policy responses developed following consultation with Australian Banking Association, ANZ, Australian Taxation Office, Bendigo Bank/Up, CBA, Google, Her Ethical AI, HMD, Match Group (Hinge), Meta, Naturalena Tech Hub, Protective Group, Service NSW, Snap, Telstra, TPG Telecom and Westpac.

[1] Department of Social Services (2022). **The National Plan to End Violence against Women and Children 2022–2032**, Department of Social Services website.

What is coercive control?

Coercive control is not one behaviour or incident, but a pattern of ongoing, repetitive, cumulative and abusive behaviour used to control someone within a relationship through manipulation, pressure and fear.[2]

When a person uses digital technologies, products and services as part of coercive control, it is known as 'technology-facilitated coercive control' or 'technology-based coercive control'.

Technology-facilitated coercive control is a complex and context-dependent form of abuse. It can involve a perpetrator exploiting vulnerabilities in technology, or misusing ordinary features within products and services, to gain and maintain power and control. This can undermine a person's confidence, freedom and independence.[3] Over time, the pattern of abusive behaviour can deprive them of their autonomy and agency.

Research suggests technology is commonly used in coercive control. For example, among a sample of women who had experienced coercive control from an intimate partner, 2 in 5 (42%) reported that their partner had abused or threatened them online or used technologies to control or stalk them.[4]

Who are the perpetrators?

Perpetrators can be of any age and from any socio-economic demographic, cultural background, ethnicity, religion or gender. However, according to research, the vast majority are male.[5] Coercive control is most commonly perpetrated by current or former intimate partners. While it is often perpetrated by men against women, it can also be perpetrated by women against men, and in same-sex relationships.[6,7,8] Perpetrators can include family members, parents, children, friends, acquaintances and strangers.[9]

---

[2] eSafety Commissioner (2025). **Coercive control,** eSafety website.
[3] eSafety Commissioner (2025). **Coercive control,** eSafety website.
[4] Boxall, H., & Morgan, A. (2021). Experiences of coercive control among Australian women. *Statistical Bulletin 30*. Australian Institute of Criminology, doi: **https://doi.org/10.52922/sb78108**.
[5] Bagshaw, D., Chung, D., Couch, M., Lilburn, S., & Wadham, B. (2000). **Reshaping Responses to Domestic Violence: Final Report**, University of South Australia.
[6] ANROWS. (2021). **Defining and responding to coercive control: Policy brief.** ANROWS website.
[7] Australian Institute of Health and Welfare (AIHW). (2018). **Family, domestic and sexual violence in Australia, 2018**. AIHW website.
[8] MacDonald, J.B., Willoughby, M., Gartoulla, P., Cotton, E., March, E., Alla, K & Strawa, C. (2024). **What the research evidence tells us about coercive control victimisation (Policy and Practice Guide).** Melbourne: Child Family Community Australia, Australian Institute of Family Studies.
[9] ANROWS. (2021). **Defining and responding to coercive control: Policy brief.** ANROWS website.

Children may also be victim-survivors in their own right, particularly where coercive control occurs between parents, and children are co-opted into the abuse.[10] Children can be affected in multiple ways:

- They can be direct victims of tactics such as tracking, monitoring and harassment.
- The tactics can be used to manipulate the child in a way that also abuses their parent or carer.
- They can be traumatised by seeing or experiencing technology-based abuse directed at a parent or carer.

For teenagers, it can also happen in their own romantic and sexual relationships.[11]

Perpetrators of coercive control often share certain attitudes, behaviours, and psychological and social drivers. However, their underlying motivations can be complex, varied and shaped by individual circumstances. While large-scale research specifically on perpetrators of technology-facilitated coercive control is lacking, qualitative research suggests motivations may include a desire for control, entitlement-based attitudes, and fear of abandonment or betrayal.[12] Perpetrators can be overt or covert in their abuse. They can also be skilled at concealing their behaviour, presenting publicly as caring while privately behaving in controlling, undermining and manipulative ways.

Attitudes that normalise coercive control

Certain attitudes and expectations can normalise technology-facilitated coercive control in intimate partner relationships. Research suggests that some young Australians, particularly young men, may struggle to distinguish between behaviours that demonstrate care and behaviours that constitute digital monitoring or control within intimate relationships.

In October 2024, eSafety surveyed 2,046 Australian adults aged 18 years and older on the extent to which they agreed or disagreed with specific online behaviours or expectations as being either a sign of care or as being reasonable within an intimate relationship.[13] The survey findings indicated the attitudes and expectations that could normalise the use of tech-based coercive control in intimate partner relationships.

---

[10] M Dragiewicz, D Woodlock, M Salter and B Harris. (2022). 'What's mum's password?': Australian mother's perceptions of children's involvement in technology-facilitated coercive control, Journal of Family Violence, 37, 137-149, 2022, doi: https://doi.org/10.1007/s10896-021-00283-4.
[11] eSafety Commissioner (2025). Supporting children experiencing domestic and family violence, eSafety website.
[12] Harris, B., Brown, C., Fiolet, R., Leins, K., & McKay, D. (2023). Technology-facilitated abuse in relationships report, The University of Melbourne website.
[13] eSafety, Investigating attitudes that normalise tech-based coercive control, eSafety website, 2024

Most participants in the survey showed some recognition that certain behaviours could be early signs of technology-facilitated coercive control in an intimate relationship. However, a sizeable proportion felt to some extent that those behaviours were usually a sign of care from a partner in an intimate relationship. Examples of this type of behaviour included checking how a partner looks in a photo before they share or post it online, constantly texting a partner to check who they are with or what they are doing when they are not together, and wanting a partner to be constantly available to respond to texts, calls or video chats.

Likewise, most participants in the survey agreed that expectations from a partner that may be indicative of technology-facilitated coercive control were unreasonable within an intimate relationship. However, a significant proportion felt to some extent that those expectations were reasonable. Examples of this included expecting to have a partner's passwords for personal devices and expecting to track a partner using location-sharing apps whenever they want.

The research found higher levels of acceptance among younger adults and men for behaviours such as messaging frequently, using location tracking, accessing passwords and requiring constant availability. This suggested that some forms of technology-facilitated coercive control may be normalised or interpreted as signs of care and concern rather than control and abuse.

These findings show why technology-facilitated coercive control needs targeted education and awareness-raising in the community. It also reinforces the need for companies to understand coercive control risks and design products and services with appropriate safeguards.

Who does it affect?

Research on coercive control more broadly can help identify who is most at risk of victimisation. While findings on demographic characteristics are mixed,[14] more recent research suggests women are more likely than men to have experienced behaviours indicative of coercive control from an intimate partner.[15] The same research found that women aged 35 to 54 were more likely to experience these behaviours than younger or older women.

---

[14] MacDonald, J.B., Willoughby, M., Gartoulla, P., Cotton, E., March, E., Alla, K & Strawa, C. (2024). **What the research evidence tells us about coercive control victimisation** (Policy and Practice Guide). Melbourne: Child Family Community Australia, Australian Institute of Family Studies.

[15] Australian Bureau of Statistics. (2021-22). **Personal Safety, Australia**. ABS website.

Demographic data from the specialist support service, Protective Group, also suggests victims-survivors are commonly aged between 30 and 55.[16]

Evidence suggests certain cohorts of women may face a higher risk of coercive control victimisation. These include:

- **Aboriginal and/or Torres Strait Islander** women
- women with **disability**
- women from **non-English speaking, culturally and racially marginalised backgrounds**
- **migrant and refugee** women and temporary visa holders
- **transgender** women
- women in **regional, rural and remote areas**
- women who have experienced **childhood maltreatment**.[17,18,19]

Coercive control can also be exacerbated by intersectional factors and experiences. This adds another layer or dimension to the abuse.

Other people and groups who may be affected include:

- **Children and other household members.** Exposure to controlling behaviours can cause significant emotional harm and perpetuate cycles of abuse.
- **Adults who experienced childhood abuse or witnessed domestic violence.** This cohort is also more likely to experience emotional abuse or coercive control in adulthood.[20]
- **People in marginalised communities.** This includes people with disability, culturally and racially marginalised people, people facing financial stress or dependency, people with limited English proficiency, LGBTIQ+ communities, and people living in rural or remote areas.
- **Older people.** Coercive control can also manifest in the context of **elder abuse,** where technology may be used to monitor, isolate, pressure or control an older person.

---

[16] Naturalena Foundation and Protective Group, consultation with eSafety, 29 September 2025.
[17] Australian Bureau of Statistics. (2021-22). **Personal Safety, Australia**. ABS website.
[18] MacDonald, J.B., Willoughby, M., Gartoulla, P., Cotton, E., March, E., Alla, K & Strawa, C. (2024). **What the research evidence tells us about coercive control victimisation** (Policy and Practice Guide). Melbourne: Child Family Community Australia, Australian Institute of Family Studies.
[19] Flynn, A., & Wheildon, L. (2024). *Technology-facilitated coercive control: Mapping women's diverse pathways to safety and justice*. Australian Institute of Criminology. **https://doi.org/10.52922/crg77536**.
[20] University of Queensland. (2025). **Coercive control puts children at risk of mental illness later in life – News – The University of Queensland**, University of Queensland website.

What are the impacts?

There is limited but evolving research on the impacts of coercive control that is specifically facilitated by technology.[21] However, evidence from studies into coercive control more broadly suggests the impacts are likely to be serious and may be similar to experiences of coercive control that do not involve technology. Victim-survivors can experience significant psychological and emotional distress, mental health issues, and feelings of fear, shame, paranoia and hypervigilance. These impacts may extend to trauma and affect future relationships.[22,23] Anxiety and fear are also common among victim-survivors who have experienced emotional abuse from an intimate partner.[24]

In a 2021 qualitative study with 15 Australian domestic violence specialists, participants highlighted the amplified fear victim-survivors can experience under constant control. Victim-survivors may feel they have no space free from a perpetrator's invasive contact or monitoring.[25,26]

Small-scale qualitative studies suggest other impacts can include social isolation, withdrawal from online life, and financial hardship, including limited or no access to finances.[27,28]

Coercive control can diminish a person's liberty and affect their perception, sense of self and autonomy. When it is facilitated by technology abusers can effectively achieve omnipresence, hindering victim-survivors from undertaking daily activities and contacting support.[29]

---

[21] Lohmann, S., Cowlishaw, S., Ney, L., O'Donnell, M., & Felmingham K. (2024). The Trauma and Mental Health Impacts of Coercive Control: A Systematic Review and Meta-Analysis, *Trauma, Violence, & Abuse, 25*(1):630-647. https://doi.org/10.1177/15248380231162972

[22] MacDonald, J.B., Willoughby, M., Gartoulla, P., Cotton, E., March, E., Alla, K & Strawa, C. (2024). What the research evidence tells us about coercive control victimisation (Policy and Practice Guide). Melbourne: Child Family Community Australia, Australian Institute of Family Studies.

[23] Flynn, A., & Wheildon, L. (2024). *Technology-facilitated coercive control: Mapping women's diverse pathways to safety and justice*. Australian Institute of Criminology. https://doi.org/10.52922/crg77536.

[24] Australian Bureau of Statistics. (2021-22). Personal Safety, Australia. ABS website.

[25] Woodlock, D., McKenzie, M., Western, D., & Harris, B. (2020). Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control. *Australian Social Work*, *73*(3), 368–380. https://doi.org/10.1080/0312407X.2019.1607510.

[26] Fiolet, R., Brown, C., Wellington, M., Bentley, K., & Hegarty, K. (2021). Exploring the Impact of Technology-Facilitated Abuse and Its Relationship with Domestic Violence: A Qualitative Study on Experts' Perceptions. *Global Qualitative Nursing Research*, *8*(1), 233339362110281. https://doi.org/10.1177/23333936211028176.

[27] Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: women's experiences. *The British Journal of Criminology*, *59*(3), 551-570. https://doi.org/10.1093/bjc/azy068.

[28] Flynn, A., & Wheildon, L. (2024). *Technology-facilitated coercive control: Mapping women's diverse pathways to safety and justice*. Australian Institute of Criminology. https://doi.org/10.52922/crg77536.

[29] Rogers, M. M., Fisher, C., Ali, P., Allmark, P., & Fontes, L. (2022). Technology-Facilitated abuse in intimate relationships: A scoping review. *Trauma, Violence, & Abuse*, *24*(4), 152483802210902. https://doi.org/10.1177/15248380221090218.

How is technology used as part of coercive control?

Perpetrators often use multiple vectors across different digital products, platforms, and services to target victim-survivors. Their behaviour may be overt or covert.

WESNET's 2026 Third National Survey of Technology Abuse and Domestic Violence gathered responses from 307 Australian frontline family, domestic and sexual violence practitioners. They reported that 96.9% of practitioners identified coercive control as co-occurring with the use of technology in domestic violence. In addition, 68.1% saw GPS tracking and location tools being used 'often' or 'all the time', while 94.1% reported seeing abuse via social media and online platforms. Messaging apps were also a common tool for abuse, and smartphones were regularly identified as a key device enabling abuse, with 96.1% of practitioners reporting that smartphones and messaging apps were being used either 'often' or 'all the time'. Emerging technologies have also become a common tool for abuse, with 74.3% of practitioners reported seeing perpetrators use AI-generated threats and impersonation tools.[30]

While perpetrators may be sophisticated in their perseverance and approach to coercive control, they often weaponise popular technologies and features that are relatively simple or designed for other purposes. For example, they may use knowledge of a victim's personally identifiable information without their authority to create impersonation accounts. Integration of advancing technologies such as AI and the Internet of Things can also increase the risk of coercive control.[31,32,33]

---

[30] WESNET (2026). **The Third National Survey on Technology Abuse and Domestic Violence in Australia**, WESNET website.
[31] Griffiths, M. (2025). **'I felt degraded': Abusers are using ChatGPT and generative AI for coercive control**, Crikey website.
[32] Dupré, M. (2025). **Elon Musk's Grok Is Providing Extremely Detailed and Creepy Instructions for Stalking**, Futurism website.
[33] Brown, A., Harkin, D., & Leonie Maria Tanczer. (2024). Safeguarding the 'Internet of Things' for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. *Violence against Women*, *31*(5). **https://doi.org/10.1177/10778012231222486**.

Perpetrators commonly use technology to carry out coercive control through the following tactics:[34]

Impersonation Creating deepfakes, personas or fake accounts to monitor, gather information, harass a person, or produce material intended to damage their reputation or humiliate them.	**Process abuse and false reporting** Misusing safety features, processes, or portals to make vexatious requests, or using reporting tools to falsely accuse a victim-survivor of abusive behaviour.
Surveillance, monitoring and stalking Using access to devices, accounts, open-source techniques or software to monitor a person's activities or location.	**Digital sabotage, tampering and gaslighting** Using connected devices to intimidate, monitor or restrict a person's access, including by deleting files or changing configuration settings.
Overloading and volumetric attacks Using accounts, tools, bots or groups to coordinate large volumes of comments, messages or other contact, making a product or service difficult or unsafe to use.	**False information and narrative generation** Creating synthetic histories or documents (such as emails, messages or chat history) or personalised abuse material that uses false narratives to denigrate a person.
Credential abuse and account hijacking Using accounts or login credentials to impersonate a person, control their access to resources, products and services, obtain information, or cause financial abuse and hardship.	**Denial of access and lockout** Using accounts or devices to control a person's access to products and services. This can include restricting access to information, news, social media, or other forms of communication.
Abusive content and communications Using bullying, trolling, message bombardment, image-based abuse, degrading posts, threats of violence, or sexual harassment to intimidate, punish or control a person.	**Content and information leakage** Doxing a person or leaking sensitive or private information, images or videos, to embarrass, threaten or intimidate them.

[34] European Telecommunications Standards Institute (2024). TR 103 936 – V1.1.1 – Cyber Security (CYBER); Implementing Design practices to mitigate consumer IoT-enabled coercive control, ETSI website.

Perpetrators commonly carry out coercive control through the following technologies, services and products:

- **Social platforms:** Social media, gaming platforms, dating apps and messaging services may have features weaponised or abused. These platforms enable coercive control by making it easy to monitor, harass, isolate, intimidate and humliate someone continuously through messaging, location sharing, and social visibility. Perpetrators may also create imposter and anonymous accounts and use encrypted services to target a person.
- **Government, legal or administrative systems:** These online and digital services may be exploited to harass, control, intimidate, discredit or exhaust a person.
- **Online accounts, products and services:** Banking, telecommunications, delivery, ride share, food delivery, subscription services, email, digital wallets and other online accounts, products and services – especially shared and joint accounts – can be hijacked to exert control, track activities and inflict financial hardship. Login details can also be used for identity theft and credential abuse. Shared cloud storage, calendars, and photo libraries can also be use to track activities.
- **Network and communications devices and hardware:** Routers, modems and phones can be monitored and controlled. Perpetrators can also carry out carrier abuse, such as porting numbers, SIM swapping, re-enabling device tracking or changing settings.
- **Tracking devices, applications and spyware:** Perpetrators use tools such as fitness and location tracking apps and devices to monitor and stalk other people without their knowledge and consent.
- **Smart, internet-connected devices (Internet of Things):** Devices such as home assistants, security systems (cameras, locks and doorbells), home appliances, fitness and item trackers, bikes, wearables, child tracking devices and smart cars may be used to monitor movement and intimidate others.
- **Generative AI applications and automated tools:** These applications may be used to create deepfakes (such as voice or image), impersonate victim-survivors or trusted contacts, produce personalised and coordinated abuse and harassment material and create synthetic histories and documentation (such as messages, receipts and chat history) with false narratives that defame or denigrate a person. Perpetrators may also monitor conversations or use these tools to gain personal information.
- **Augmented and virtual reality hardware and software:** Can intensify coercive control by creating immersive experiences that make monitoring, harassment, and intimidation feel constant and inescapable, reinforcing control even when the perpetrator is physically absent.

Potential signals of coercive control

Perpetrators often use tactics or technology that may not appear suspicious to people outside the relationship. These can include devices and apps that are part of ordinary daily life. This can make technology-facilitated coercive control difficult to monitor and detect accurately. The harm can also escalate over time, making it hard for victim-survivors to seek help, regain control or use products and services safely.

Patterns of behaviour can be misunderstood without the right context. There is also no universal typology for identifying signs of technology-facilitated coercive control, which means companies often rely on users, law enforcement and other trusted sources to understand what may be occurring.

Context is critical. Potential signs of coercive control, whether user-reported or detected by an organisation, may include:

- changes to login, account or configuration settings, contact details or preferences without a person's knowledge or consent
- unauthorised access to online accounts, services, devices or information
- pressure to provide access to accounts or devices or forced creation of authorised representatives
- forced password or credential sharing, intercepted one-time passwords (OTP) or repeated password or account recovery attempts
- identity impersonation, identity theft or the creation of fraudulent accounts
- online threats, vexatious reports, abusive posts or false accusations
- parental controls used on adult devices or accounts
- unauthorised requests to close, cancel or disconnect accounts and services, or refusal to close accounts
- online withdrawals or other transactions made without a person's knowledge or consent
- communications or digital correspondence not being received
- location, communications or spending history tracked through real-time notifications or monitoring
- controlled or restricted access to accounts, services or devices
- changed plans or subscriptions, including unaffordable or unauthorised purchases.

Sector specific

Banking and financial services[35]	**Energy, utilities and resources**[36]	**Telecommunications**
• Abusive messages sent through online payment descriptions • Controlled or restricted access to finances • Money or assets used without consent • Forced debt, including loans or credit cards taken out without consent	• Energy usage patterns tracked • Controlled or restricted access to accounts, services and appliances	• Unwelcome communications via calls, SMS or MMS • SIM change requests, including unauthorised SIM changes or SIM swapping • Location, internet usage, or communications monitored • Internet services disconnected
Digital platforms and services	**Consumer technologies and devices**	**Government systems**
• Controlled or restricted access to news, information and social media • Message bombardment • Synthetic histories or documents, such as messages, emails and chat histories • Threats, bullying and trolling via messages, calls and posts • Private, sensitive or personal information posted online	• Settings and controls on Internet of Things (IoT) and smart home devices • Unknown tracker alerts or hidden trackers • Recording or filming without consent • Unusual battery drain • Persistent unknown background apps • Files or data deleted without consent	• Welfare, benefits or assistance applications made via online portals without knowledge or consent • Superannuation withdrawals made without knowledge or consent • Government refunds or payments redirected or withheld • Controlled or restricted access to identification documents or systems

Evolving tactics

Coercive control tactics continue to evolve as perpetrators adapt everyday technologies, connected devices and digital services to monitor, isolate, intimidate and control victim-survivors.

Emerging and evolving tactics include:

- **Spyware disguised as parental controls:** Spyware and stalkerware can be installed under the guise of parental controls, masking their true intent and making detection difficult.[37]

[35] Flequity Ventures (2022). Design to Disrupt – Reimagining banking products to improve financial safety, Design to Disrupt website.
[36] Flequity Ventures (2025). Safety by Design for essential services, Design to Disrupt website.
[37] Naturalena Foundation and Protective Group, consultation with eSafety, 29 September 2025.

- **Exploitation of parental controls, apps and family management software:** Parental controls within digital products and services alongside child safety apps and family management software can be used to monitor and track individuals through geofencing alerts, mirroring and live location mapping. It can also be used to restrict access to resources and isolate individuals through limit settings, blocking controls and filters. Children's devices can also be used as proxy trackers and as coerced intermediaries.[38]
- **Compromised devices:** Safe phones can be compromised through unauthorised access to linked Google accounts, enabling GPS tracking and data extraction.[39]
- **Unauthorised tracking devices:** Connected tracking devices are often hidden in cars, sometimes with multiple devices placed in one vehicle, to monitor movements without consent.[40] Data from Protective Group, a technical specialist support service, states that it finds up to six 'tile' devices each week on vehicles across Australia.[41] Children's toys, pet trackers and personal possessions have also been used to hide tracking, listening and video recording devices. The NSW Crime Commission's June 2024 Project Hakea report also found an increase in tracker purchases and evidence of frequent use of tracking devices by domestic and family violence perpetrators. It found that nearly 25% of known individuals who purchased tracking devices since 2023 had a history of domestic violence.[42]
- **Exploitation of location tracking apps:** Real-time sharing and location tracking features can be available in apps for purposes such as family safety, fitness, device and item tracking, travel logging, navigation and delivery. These apps can be used to monitor a person's movements and location, where a perpetrator can stalk them without their knowledge and consent.[43,44]
- **Exploitation of smart connected devices (Internet of Things):** Smart and connected devices, such as home assistants, appliances, wearables, child tracking devices, energy tracking devices and software, security systems, cameras, locks, doorbells and smart cars, can be used to monitor movement, intimidate victim-survivors and cause isolation.
- **Financial abuse:** Perpetrators may use coerced debt, business coercion, money muling, accounts weaponised after separation, misuse of power of attorney, and micro transactions to send messages via transaction description fields in online banking

---

[38] Irving, M., & Boxall, H. (2026). Post-separation Parenting Apps as Tools for Control and Resistance. Violence Against Women. 13:10778012261429100. https://doi.org/10.1177/10778012261429100.
[39] Naturalena Foundation and Protective Group, consultation with eSafety, 29 September 2025.
[40] Naturalena Foundation and Protective Group, consultation with eSafety, 29 September 2025.
[41] Protective group (2024). Disturbing ways technology is used to control and track domestic violence victims, Protective Group website.
[42] NSW Crime Commission (2024). HAKEA Final Report 25 June 2024.pdf, NSW Crime Commission website.
[43] Levy, A. (2025). Location-sharing apps linked to increased risk of digital coercive control, eSafety Commission research finds – ABC News, ABC News website.
[44] Zemek, S. (2025). Paul Thijssen: Inside the life of twisted Lilie James killer, News.com.au website.

platforms and apps. NSW Police recorded 473 incidents of coercive control between 1 July 2024 and 31 December 2025, with 52% involving financial abuse, an increase of 7% from the previous year.[45]

- **Telecommunications abuse:** Perpetrators may use number porting, joint accounts takeovers, unwanted communications and shared plans to monitor or isolate victim-survivors. A report from Victoria's Sentencing Advisory Council found that harassment and abuse through a telecommunications service accounted for more than one-third of all federal crimes sentenced in Victoria's courts.[46]
- **AI misuse and abuse:** Perpetrators may use AI services to create deepfakes and use them for sexual image-based abuse. This may include face swapping content, making people appear undressed or nude, making people appear to not be wearing cultural and religious attire, and voice cloning. Perpetrators can then threaten to share the material, gain access to personal information to use for stalking, and generate false histories and evidence.[47,48] Conversational, generative and agentic AI tools can also be weaponised to facilitate, scale and automate coercive control tactics such as harassment, bullying, surveillance, tracking, stalking, controlling and restricting access to resources. The Queensland Centre for Domestic and Family Violence Research released an insights report suggesting generative tools present significant risks to victim-survivors and can intensify established patterns of coercive control.[49]
- **Misuse and abuse of delivery apps:** Perpetrators may weaponise parcel delivery and food delivery app accounts to track, monitor, verify or infer routines, movement and presence at a location.[50] Through sending items and tracking histories, perpetrators are able to verify a person's location and maintain control without needing to be physically present. Perpetrators can also misuse delivery services through redirection and interception of deliveries, packages and items, embedding hidden tracking devices into packages and using delivery app data to monitor victim-survivors' ordering history, delivery patterns, and locations.

---

[45] BOCSAR (2025). **Coercive control monitoring reports,** BOCSAR website.
[46] Sentencing Advisory Council Victoria (2026). **Commonwealth Offences Sentenced in Victoria**, Sentencing Advisory Council website.
[47] Griffiths, M. (2025). **'I felt degraded': Abusers are using ChatGPT and generative AI for coercive control**, Crikey website.
[48] Dupré, M. (2025). **Elon Musk's Grok Is Providing Extremely Detailed and Creepy Instructions for Stalking**, Futurism website.
[49] D'Rosario, M. (2026). **Artificial Intelligence, Coercive Control, and Foreseeable Risk in Domestic and Family Violence Contexts,** No Violence website.
[50] Zemek, S. (2025). '**Paul Thijssen: Inside the life of twisted Lilie James killer**', News.com.au website.

Applications of Safety by Design across sectors

Safety by Design approaches are already being applied in family, domestic and sexual violence and technology-facilitated abuse contexts. These approaches offer practical lessons for addressing coercive control across different sectors. The Australian Government is also working to apply the principles of Safety by Design to systems reform and design, to contribute to preventing abuse of Commonwealth systems, as part of recommendations from The Rapid Review of Prevention Approaches.[51] The review highlighted that Safety by Design principles may have broader application in preventing coercive control and other forms of abuse beyond digital platforms, including through the design of government systems. The review also noted the importance of embedding safety considerations and harm prevention within government systems, services and industry practices.

Sector-specific

Banking and financial services	**Telecommunications**
• Embedding Safety by Design into product development, governance and staff training • Trialling fraud controls to detect and prevent financial abuse • Developing AI tools to proactively detect financial abuse • Updating terms and conditions to set out customer responsibilities and relevant conditions including consequences for misuse • Creating specialist support teams that provide trauma-informed and tailored support for people experiencing abuse • Conducting product safety and risk assessments • Adapting three lines of defence and risk models to address abuse • Embedding lived-experience insights and customer touchpoints into product development lifecycles	• Implementing internal and external processes, measures and controls that align with domestic violence standards • Exploring proactive flagging systems and call monitoring to identify patterns of abuse • Tracking how often customers report issues or incidents • Training staff to identify abuse and subtle warning signs without alerting perpetrators

[51] Department of the Prime Minister and Cabinet (2025). Theme 5: Prevention through systems and industries | Rapid review of prevention approaches: Australian Government implementation update –30 October 2025 | PM&C, Department of the Prime Minister and Cabinet website.

AI and safety tech	**Digital platforms and services**
• Building explainable, privacy-first tools for detection and support • Collaborating with victim-survivors, people with lived experience, law enforcement and legal experts to improve justice outcomes	• Enhancing user controls, reporting mechanisms and transparency measures • Monitoring the use and potential misuse of location-sharing features, including how they may create risk in specific contexts

Examples of how technology companies are taking a Safety by Design approach to coercive control remain relatively limited. This is due to a range of factors, including the nuanced nature of coercive control, difficulties in detection, and privacy considerations. Despite these challenges, progress is being made, with technology companies exploring design interventions, response frameworks and other measures to address coercive control.

Considerations with implementation

Technology-facilitated coercive control is complex, context-dependent and often dynamic, which can raise challenges in accurate detection and appropriate response. The patterns of abuse are not always easy to quantify and sometimes lack clear markers or signals. As a result, coercive control can be misread or missed by automated systems, individuals and teams.

Perpetrators also adapt and misuse products and services even where safeguards are in place. Limited awareness, underreporting and inconsistent issue recognition of technology-facilitated coercive control can also mean it is not treated as a prioritised harm type.

Key challenges and considerations include:

- **Automated detection:** AI-driven tools can struggle to distinguish coercive control from ordinary and authentic interpersonal behaviour or engagement. This can result in **false positives and false negatives**. Over-reliance on automated detection can lead to misclassification, damage trust and undermine the user experience. Care must be taken to avoid over-reliance on automated detection.
- **Language evasion:** Perpetrators frequently use **language evasion to avoid detection**. This can include digital linguistic art (algospeak), such as acronyms, coded words, images or emojis that appear harmless but carry threatening or abusive meaning for the intended target. For example, a flame emoji may casually suggest someone is attractive, but in a context where a perpetrator has threatened to burn down a family home, it could instead convey an implied or indirect threat. This deliberate obfuscation makes it harder to keep pace with evolving patterns of abuse. Companies need to account for these changing patterns of abuse in their safety approaches.

- **Privacy and data protection laws and regulations:** Privacy laws and data protection regulations can **limit the ability to share** information across platforms and institutions. These laws protect user rights, but they can also hinder coordinated responses, especially when abuse spans multiple services or jurisdictions. Companies should consider a balanced approach to adopting safety and privacy-preserving approaches that support regulatory compliance and proactive user safety.
- **User reporting and underreporting:** Due to legal requirements and compliance obligations or restrictions, **companies often rely on user reporting** and have limited visibility over interactions, making proactive detection and intervention challenging. Companies also tend to rely on user reporting to avoid over enforcement, as individual circumstances and context are important. Underreporting can also be driven by safety concerns, fear of retaliation, shame, lack of trust in reporting systems and a victim-survivor's emotional ties to the perpetrator. Reporting processes should be trauma-informed and guided by lived experience.
- **Perpetrator adaptation:** Perpetrators often find new ways to misuse products and services. Even well-designed safeguards can be bypassed through creative exploitation or **circumvention of controls and measures**. Companies cannot anticipate every abuse scenario, but they can continually conduct abusability testing across products, services, features and functions.
- **Legacy systems and complex infrastructure:** Older platforms, **legacy** systems and historical products as well as **difficult and complex processes and programs** often lack the flexibility to implement modern safeguards. Retrofitting these systems with measures can be costly and technically challenging, leaving gaps for exploitation. Companies should consider what safeguards can be built into existing systems and infrastructure, as well as streamlining processes and programs.
- **Proactive detection:** Detecting technology-facilitated coercive control before harm occurs is one of the greatest challenges. Unlike more overt forms of abuse, coercive control often manifests through patterns of behaviour over time and companies may not have visibility over offline dynamics. This requires contextual understanding and, where appropriate, analytics that can identify patterns rather than isolated incidents. It is also difficult to identify through behavioural indicators, analytics, or data alone without direct engagement with victim-survivors and disclosure. Companies should establish processes to detect and act on coercive control-related behaviour with the aim of preventing or reducing harm.

- **Risk of unintended harm:** Measures and controls may support and protect users in certain scenarios but increase risk of harm in others. A 'Do No Harm' approach can help ensure well-intentioned actions do not inadvertently exacerbate harm.[52]
- **Lack of shared indicators:** There is **no universally accepted typology** or set of indicators for coercive control in digital environments. This lack of standardisation makes it difficult for companies to design consistent policies, train staff, and develop interoperable detection tools. Furthermore, there is inconsistency across the ecosystem, sectors and related research in the **terminology, definitions and scope** of what are considered coercive behaviour and signals. Shared language and understanding can improve data and research and provide a clearer picture of the issues and how they occur.
- **Training and awareness:** Training staff to recognise and respond to technology-facilitated coercive control can be difficult because the abuse is often complex, contextual, lacks clear identifiers and is poorly understood. Staff may need to understand how technology is misused, how perpetrators maintain control, how to identify signs of coercive control, how intersectional factors may affect risk and how to support victim-survivors safely. Training should be co-designed with experts so staff can recognise, respond, refer and provide support in the moment.

Practical measures to address coercive control

Many ways to address technology-facilitated coercive control are closely linked to, or build on, existing Safety by Design measures for technology-facilitated gender-based abuse.

Responses to coercive control should be victim-survivor-centred and flexible enough to respond to different needs and experiences. Companies should embed lived-experience insights and trauma-informed practice from the outset.

Controls, mitigations and processes can support and protect victim-survivors in some cases but increase risk in others. This is because victim-survivors may have different experiences, face different risks, impacts and be navigating complex circumstances.

[52] UNFPA (2024). A Survivor-Centred Approach to Monitoring Gender-based Violence Response Programming, UNFPA website.

A 'Do No Harm' approach can help companies identify and mitigate the risk of unintended consequences, so well-intentioned interventions do not inadvertently make harm worse.[53]

Companies should also understand technology-facilitated abuse as an extension of existing domestic violence behaviours including coercive control, rather than a unique set of behaviours.[54]

Victim-survivors have often already experienced a loss of control. If they are not able to make decisions about their own online experience, they may be subjected to another form of control.[55] Companies have a responsibility to ensure the burden of safety does not sit with victim-survivors. The right response places responsibility with service providers to embed safety into product and service design, processes, controls, and responses while preserving victim-survivors' autonomy and decision-making. Feasibility, relevance, and appropriateness of approaches, measures and responses will differ across sectors.

Service provider responsibility

Service providers can play a central role in preventing and responding to coercive control. This means building clear protocols, detection processes, controls and safety protections into products, services and internal systems from the outset.

1. Develop clear protocols and procedures

Ensure clear protocols are in place for responding to coercive control and engaging with law enforcement and support services. Policies, procedures and guidelines should be documented, trauma-informed and designed to prioritise user safety. Consider:

- protocols that uphold the privacy and safety of victim-survivors, including how their privacy will be protected
- record-keeping requirements for handling and disclosing information
- how actions agreed with a victim-survivor will be recorded safely, including when those actions are completed, without inadvertently disclosing information to perpetrators
- how policies and procedures apply to both perpetrators and victim-survivors

---

[53] UNFPA (2024). A Survivor-Centred Approach to Monitoring Gender-based Violence Response Programming, UNFPA website.

[54] Fiolet, R., Brown, C., Wellington, M., Bentley, K., & Hegarty, K. (2021). Exploring the Impact of Technology-Facilitated Abuse and Its Relationship with Domestic Violence: A Qualitative Study on Experts' Perceptions. *Global Qualitative Nursing Research*, *8*(1), 233393362110281. https://doi.org/10.1177/23333936211028176.

[55] Davies, J., Lyon, E., and Monti-Catania, D. (1998). Creating the image of battered women. In *Creating the image of battered women* (pp. 11-20). SAGE Publications, Inc., https://doi.org/10.4135/9781452232034.n2.

- what processes and measures are in place to protect and support victim-survivors
- what escalation and triaging pathways exist and how staff will know when to use them
- how staff can safely and appropriately engage with other parties
- how victim-survivors will be identified and supported, and how cases will be managed
- how inclusive design will be used during the development and review of products, services and processes to identify and reduce risks and harms
- staff responsibilities when dealing with victim-survivors.

2. Implement detection processes

Establish processes to detect and act on coercive control-related behaviour with the aim of preventing or reducing harm. This may include:

- deploying technologies similar to fraud detection, monitoring and behavioural analytics, adapted to coercive control that is facilitated by technology. At-risk demographic factors should be considered alongside behavioural and situational indicators, such as a history of domestic or family violence, social isolation, financial dependence, and access to support services. These approaches may include:
    - using fraud detection technologies to identify unauthorised, deceptive, criminal or suspicious activity through data signals, rules, behavioural analysis, pattern analysis, analytics, AI and machine learning to detect anomalies and deviations from normal, standard or expected behaviour. Many indicators of coercive control can also resemble fraud signals
    - applying these tools in a coercive control context to reveal patterns of financial abuse, impersonation, unauthorised actions or coercive account activity that may indicate ongoing control or abuse of a victim-survivor
- using account monitoring, behavioural analytics and analysis
- training staff to identify abuse patterns and coercive behaviours
- using feedback loops in reporting processes to improve the accuracy of detection tools.

3. Conduct risk management and testing

Consider adapting a ‘three lines of defence’ model for abuse, with operational, risk management and independent assurance functions. Inclusive design and safety should be built into the product development lifecycle. This includes considering at-risk users, touchpoints, stress testing, training product owner training and risk and safety assessments at all stages.

Key considerations include:

- maintaining a risk register and develop and monitor controls and measures
- developing a range of user personas, journeys and profiles
- ensuring user research guides are key to decisions and are understood by development teams
- reviewing complaints and incidents to identify how products and services are being misused
- conducting usability and abusability testing from both perspectives: the person who may use the product or service to cause harm and the person who may experience that harm
- conducting safety impact assessments
- using complaints data to understand new and emerging risks
- developing and evaluating test cases, including how abuse could occur in different circumstances, such as during a relationship, at the point of separation and after separation, noting that each stage can create different dynamics and risks.

Consider the following questions:[56]

- Could specific features, functions or controls, create personal safety risks or make a situation worse?
- Does the design create risks of control or abuse, intentionally or unintentionally?
- Can the product or service be designed to reduce these risks from the outset? If not, what controls can be put in place to mitigate the impact?
- Can the design, measures and controls help a victim-survivor recognise that abuse is occurring through the product or service, understand what they can do about it, and access support?
- Can the design help identify user activity that may indicate abuse, including patterns unique to a user or coercive behaviours by a perpetrator?

4. Consider security, privacy and safety

Integrate security, privacy and safety into product and process development, alongside case management processes.

[56] European Telecommunications Standards Institute (2024). **TR 103 936 – V1.1.1 – Cyber Security (CYBER); Implementing Design practices to mitigate consumer IoT-enabled coercive control**, ETSI website.

This may include:

- obscuring account and contact details for at-risk users so staff do not inadvertently provide details to perpetrators
- removing non-essential personal data from notifications and correspondence
- creating a separate workflow or process with additional safety protections for users who have disclosed abuse
- making information about support options readily available without requiring users to ask
- collecting only necessary information and storing it securely, with access controls based on the principle of least privilege
- not requiring at-risk users to disclose the circumstances of the abuse as a precondition for accessing support
- establishing reporting processes that minimise the need for users to explain their circumstances multiple times
- establishing reporting and information handling mechanisms which uphold victim-survivor privacy and do not alert the perpetrator
- developing protocols that address how privacy and safety will be prioritised in joint or shared accounts, where relevant.

Case study: Embedding Safety by Design into product governance[57]

Evidence from the financial sector and lived-experience insights show that banking products can be misused to enable coercive control.

To better understand where those risks could arise, CommBank examined customer interactions, customer journeys and insights from lived-experience workshops.

CommBank responded by embedding Safety by Design into its product governance lifecycle, shifting from a reactive approach to a preventative one. Safety by Design considerations were incorporated into product governance templates, requiring teams to explicitly assess new products for potential misuse, and consider what safeguards may be needed to reduce the risk of misuse.

[57] CBA, consultation with eSafety, 12 September 2025.

To support this work, CommBank developed a Safety by Design Agent. The tool assists product teams in identifying risks, applying Safety by Design prompts and generating mitigation actions to reduce harm during design, assessment and review.

CommBank also partnered with a specialist not-for-profit organisation to deliver trauma-informed, co-designed workshops with lived-experience advisors. These workshops used personas, journey mapping and scenario testing to stress test the development of potential new products.

The result is a more consistent way to build safety into product development. This approach embedded Safety by Design as a governance standard rather than an individual capability, as part of how products are assessed and updated. The work has led to the inclusion of effective interventions into a number of products and services, demonstrating how governance-led design can reduce harm while improving safety and inclusion.

The CommBank example shows how a large service provider can move from responding to harm to changing products and services processes to make abuse harder to enable.

User empowerment and autonomy

Victim-survivors should be supported to make informed choices about their own safety and online experience. Safety features should increase user autonomy and reduce risk without placing the burden of safety on the person experiencing abuse. Balancing how and when to surface support without diminishing a user's control and agency is key.

1. Incorporate safety measures into the user experience

Inclusive design and safety measures should account for at-risk users, journeys, personas and touchpoints. User controls, guardrails and empowerment are central to managing risk. These are some examples:

- Positive friction, such as through authentication methods and additional steps to confirm if actions are authentic, and reporting mechanisms that trigger automatic refusals where appropriate. These processes should be designed with careful attention to both benefits and risks, as additional steps may hinder victim-survivors or alert perpetrators.

- Indicators and notifications that show when features and functions have been activated and are collecting information.[58]
- Reminders and notifications about authentication, who is on the network or who has access, supported by comprehensive session-management details. Notification features should be designed carefully, as they may also alert perpetrators.
- Replacing 'set and forget' features with ongoing notification and reauthorisation protocols, and promoting awareness of granted legacy permissions.[59]

2. Provide human-guided, trauma- and safety-informed support

Consider providing non-automated support that can empower and assist users. Ensure the following:

- Safety and privacy are both considered when cases are escalated.
- Victim-survivors' experiences and choices are validated without judgement.[60]
- Communications are delivered in a way that minimises the risk of a victim-survivor feeling compelled to follow advice. They should instead support and empower the victim-survivor to understand that they are best placed to decide what is right for them.
- Advice to delete accounts or disengage from technology is treated with caution. It may not be viable, may cause isolation, and may place the burden on the victim-survivor to change their behaviour.
- Advice and controls that inform decision-making without trying to influence or override the user's choices.[61]

Case study: Tackling payment abuse through a user-centric approach[62]

Perpetrators of coercive control often use low-value payments to keep contacting victim-survivors as a workaround after they have been blocked on other platforms. Harassing messages can be hidden in payment descriptions, turning a banking feature into another way to intimidate, monitor or maintain control.

---

[58] Brown, A., Harkin, D., & Leonie Maria Tanczer. (2024). Safeguarding the 'Internet of Things' for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. *Violence against Women*, *31*(5). **https://doi.org/10.1177/10778012231222486**.

[59] Brown, A., Harkin, D., & Leonie Maria Tanczer. (2024). Safeguarding the 'Internet of Things' for Victim-Survivors of Domestic and Family Violence: Anticipating Exploitative Use and Encouraging Safety-by-Design. *Violence against Women*, *31*(5). **https://doi.org/10.1177/10778012231222486**.

[60] Flynn, A., & Wheildon, L. (2024). *Technology-facilitated coercive control: Mapping women's diverse pathways to safety and justice*. Australian Institute of Criminology. **https://doi.org/10.52922/crg77536**.

[61] IBM Policy Labs (2020). **Coercive Control Resistant Design**, IBM website.

[62] Bendigo Bank and Up, consultation with eSafety, 6 October 2025.

Up, a subsidiary of Bendigo Bank, identified this pattern through internal research. It found that approaches such as keyword blocking or automatic account closure, used on their own, were not enough to stop the abuse. In some cases, they could also create new risks by restricting victim-survivors' financial access. Up therefore strengthened its response to prioritise customer safety while preserving autonomy.

Up implemented behavioural account monitoring to detect potentially abusive transaction descriptions. As blocking payments can negatively impact access to essential funds, Up introduced a 'Muting and Redaction' feature. This allows customers to continue receiving payments while abusive text is automatically replaced with a neutral placeholder: 'Message removed'.

Customers can also remove payment descriptions and payee names from their transaction history and statements. This gives them more control over what they see in their own banking records, without forcing them to close accounts or lose access to essential funds.

Up introduced further safety features, including:

- privacy controls that let customers limit whether others can find or identify them as an Up customer
- alternatives to account closure, such as issuing new PayIDs
- options to remove abusive content from activity feeds
- blocking and unblocking tools to prevent further payments and messages
- warning notifications where abusive behaviour is detected.

Up also issues warning notifications when it detects abusive behaviour. Perpetrators have one day to respond and comply. If the behaviour continues, or there is no response, accounts are closed in line with Up's terms and conditions.

In financial year 2024–25, Up reviewed 30,112 payments, resulting in 1,187 accounts being flagged for abuse or closure and 493 abuse warnings being issued. Since Up introduced in-app blocking and muting features, manual abuse reports have significantly decreased.

Up's story and model of combining automated detection, graduated enforcement and customer and controlled safety features shows how banks can disrupt abusive communication without cutting victim-survivors off from financial access and without compromising autonomy. It also shows the value of designing safety features that give customers more control, rather than forcing them to choose between staying connected and staying safe.

Case study: User safety features on dating platforms[63]

Research shows that online harassment has been on the rise across all digital spaces, particularly for underrepresented and high-risk groups.[64] When it comes to online dating platforms, women, LGBTIQ+ people and those from culturally and linguistically diverse backgrounds can experience harms such as technology-facilitated gender-based violence and coercive control at disproportionately high rates. Online dating platform Hinge took a Safety by Design approach by combining platform-level harm reduction with customisable features, so that users are empowered to create an experience that feels right for them. By anticipating potential risks, incorporating user feedback and collaborating with affected communities, Hinge found a way to improve safety for its users.

Technical interventions by Hinge

When using Hinge, users have the option to add comments when they 'like' an image, video or answer on another person's profile. Hinge introduced 'Comment Filter' to its app to help reduce the amount of unwanted comments daters may receive before an interaction begins. The comment filter uses an AI-powered content detection model to automatically detect and hide potentially harmful comments within incoming likes before the recipient sees them. Users are only exposed to a flagged comment if they choose to review it in their 'hidden likes' section. The filter is on by default for all users and senders are not notified when their comment has been hidden. As not all users have the same safety needs, they can choose to personalise their filter by adding custom words, phrases or emojis, and can review or delete filtered content at any time. This supports users by reducing exposure to harmful, harassing and triggering language before it escalates and reaches them. This feature reflects Hinge's approach of pairing platform-level protections with user choice, empowering users to take control of their experience, while curating safer interactions.

Another safety feature implemented by Hinge is 'Block People You Know'. This feature addresses the potential for technology platforms to be used for intimate partner stalking, where a perpetrator may attempt to use an app to make contact with someone they already know. The feature allows users to prevent specific people from appearing in their feed, as well as finding and contacting them by identifying certain device contacts or entering phone numbers and email addresses manually. Blocked contacts receive no notification, protecting the user from potential identification or harassment, and a

[63] Match Group (Hinge), consultation with eSafety, 1 July 2026.
[64] Vogel, E. (2021). The State of Online Harassment, Pew Research Center website.

manual entry option lets users get protection without sharing their entire contact list with the app. By limiting access and reducing opportunities for unwanted contact, the feature reinforces users' autonomy, privacy and sense of safety.

Transparency and accountability

Transparency and accountability turn good intentions into sustained action. For service providers, this means training staff to recognise and respond to coercive control, working with experts and advocates, and sharing insights to strengthen safety across the technology ecosystem.

1. Integrate the risk of technology-facilitated coercive control into training

Co-design training with experts so staff can recognise, respond safely, make appropriate referrals and provide support in the moment. Training should be tailored to staff roles and cover:

- how to identify people affected by coercive control, including recognising abuse and subtle warning signs without alerting perpetrators
- how intersectional issues may affect at-risk users
- the norms and drivers of gender-based violence that underpin coercive control
- how to engage with victim-survivors, including when their circumstances change, while prioritising their safety
- what trauma-informed language means, with examples of how to use it and highlighting its importance
- broader risks beyond the immediate issues victim-survivors present, including processes for sharing safety resources and making referrals
- the definition and prevalence of coercive control, including how technology is misused
- scenarios and case studies showing how technology can be exploited and how staff should respond.

2. Collaborate with experts and advocates

Partner with subject matter experts, victim-survivor advocates, family and domestic violence services, and key stakeholders to co-design policies and develop, interpret and apply safety standards. These partners can provide valuable insight into gaps in safeguards, inform solutions, guide response strategies, and support culturally responsive approaches

for diverse communities. Engaging people with lived experience should always be trauma informed.[65] Companies should also consider implementing a trusted partner or flagger program which allows expert NGOs to play an important role in assessing and providing context and support. Additionally, companies should consider collaborating with family and domestic violence services for support pathways and promote external support resources and services to victim-survivors.

3. Share insights across sectors

Consider information-sharing mechanisms between organisations and sectors. Device manufacturers, app stores and developers should also collaborate to integrate safety features effectively. Sharing insights on failures, gaps and lessons learned can improve collective understanding and strengthen sector-wide responses to coercive control.

Case study: Cross-platform defences against covert location tracking[66]

Bluetooth Low Energy (BLE) tracking tags, designed for purposes such as to help users find lost keys or luggage, can be misused for physical stalking, surveillance, control and coercion. Perpetrators place these tags in places such as a victim's vehicle, bag or coat pocket to track their movements in real-time, often without their knowledge or consent. As these trackers can belong to different technical ecosystems, victim-survivors may be unaware that tracking tags designed for other operating systems are present nearby.

Intervention and tools by Google

Google proactively pursued industry-wide collaboration to address the issue of physical surveillance via BLE tags:

- **Interoperable standards:** Google collaborated with other major operating system engineers to establish a unified protocol[67] for Bluetooth tracking devices.
- **Built-in protection and integrated detection:** Android's detection capabilities were built directly into the device's operating system's firmware, meaning users do not need to download a separate application to be protected.

Google has also added a comprehensive suite of 'unknown tracker alerts' into Android:

- **Automatic background scanning:** Android scans for unknown tracking devices moving with the user. Users receive a prompt alert if an unknown tracking tag is detected

[65] Every, K. (2023). '**Applying trauma-informed principles to user-centred design**', Medium website.
[66] Google, consultation with eSafety, 1 July 2026.
[67] Ledvina B., Eddinger Z., Detwiler B., & Polatkan S. (2026). **Detecting Unwanted Location Trackers**, IETF website.

travelling with them whilst separated and moving away from its owner for a period of time.

- **Visual proximity mapping:** Users can see a map showing exactly where the tracker was first detected travelling alongside them, and the path it has followed them on.
- **Manual precision tools:** Users can initiate a 'manual scan' of their immediate surroundings at any time.
- **Tracker identification and disabling guides:** The feature enables the user to 'ring' the unknown tracker to locate it and can provide additional information, such as the device ID or serial number. The feature also presents step-by-step instructions on how to physically disable the tag's battery. Having notifications to identify unknown trackers can better support victim-survivors by allowing them to bring information, such as the tag's serial number, to local law enforcement agencies to investigate further.

Google learned the following lessons from this industry-wide collaboration and through implementing features:

- **Collaboration is essential:** It is not sufficient to have a standalone solution if it does not work across different operating systems – perpetrators exploit gaps between ecosystems. Aligned industry standards are essential to minimising 'blind spots' in physical tracker detection.
- **Care in alerting:** Care must be taken so that notifications help locate BLE tags without causing audible alerts that could put a victim in immediate physical danger while in the presence of a perpetrator.

Google measured the success of the initiative by its ability to identify BLE tags regardless of their manufacturer. Millions of Android users now have a protection measure in place that works with compatible tags, supporting the detection and prevention of covert tracking and surveillance across the ecosystem. Google has helped to empower users with transparency, cross-platform and privacy protection, as well as support in reporting processes, and ultimately, the ability to detect and disable unwanted tracking devices.

Responding to technology-facilitated abuse: eSafety's Technology-Facilitated Abuse Support Service

Initiatives and programs such as eSafety's Technology-Facilitated Abuse (TFA) Support Service play an important role in strengthening the broader support ecosystem. The service provides specialist support to frontline workers across the family, domestic and sexual violence sector, strengthening their capability to recognise and respond to technology-facilitated abuse.

The TFA Support Service delivers tailored guidance, practical advice and step-by-step support on digital technologies and online platforms. This includes assisting frontline workers to identify and respond to risks such as digital tracking, harassment and surveillance, while equipping them with strategies to reduce harm and enhance client safety. eSafety's TFA Support Service also provides insights, learnings and emerging trends with industry organisations to inform and strengthen relevant initiatives and support broader system responses.

Case study: Keeping victim-survivors safely connected[68]

One example of how industry is responding in practice to technology-facilitated abuse is through Telstra's Safe Connections program.

Perpetrators of coercive control often restrict access to devices and communications to exert control and deprive a victim-survivor of freedom, independence and autonomy. This can include restricting or confiscating phones, monitoring apps, calls and messages, or limiting who a victim-survivor can contact.

When perpetrators control access to communication, they make it harder for victim-survivors to seek help, stay connected to support networks or communicate safely with trusted people.

In response to the prevalence of this tactic, Telstra partners with WESNET to support victim-survivors experiencing domestic and family violence to stay safely connected through the Safe Connections program.

The Safe Connections program began in 2014 as a partnership between Telstra and WESNET, the national peak body for specialist domestic and family violence services. Telstra provides prepaid smartphones, pre-paid credit, network access and operational

[68] Telstra, consultation with eSafety, 7 October 2025.

support to victim-survivors. WESNET, with grant funding from the Australian Government Department of Social Services, coordinates delivery through its national network of more than 300 specialist domestic and family violence services.

WESNET provides specialist training to the agencies in the national network to ensure that victim-survivors receive devices as part of a survivor-led risk and safety plan. This training also helps practitioners and victim-survivors recognise and disrupt technology-facilitated abuse, including coercive control, and stay connected safely.

The program also addresses a practical barrier. In Australia, customers must verify their identity when activating a pre-paid mobile service. Victim-survivors fleeing family violence may not have access to their identity documents. Safe Connections allows them to activate a pre-paid mobile service and gives them 90 days to provide identification. Phone activation and ID verification are managed through Telstra's specialised Safe Team.

Telstra works closely with WESNET to adapt the program as needs change. This includes refining device kits, improving guidance materials, reviewing device allocations and strengthening impact measurement. Program insights inform Telstra's broader approach to supporting vulnerable customers and shape standards across the telecommunications sector.

By financial year 2024–25, the partnership had distributed more than 50,000 smartphones since inception. Safe Connections shows how long-term partnerships and collaboration can support service providers respond to coercive control in practical ways and enable meaningful outcomes. By combining telecommunications support with specialist domestic and family violence expertise, the program helps victim-survivors stay connected to support services and people they trust.

Conclusion

Safety by Design gives companies a practical way to reduce the risk of their products and services being misused for technology-facilitated coercive control. This chapter encourages industry to look closely at where coercive control can be enabled across products, policies, systems and support pathways – and to build safeguards before harms occur. No single product, service or sector can address coercive control alone. However, every service provider can take practical steps to make abuse harder to carry out, easier to identify and safer to manage when it happens. We encourage all tech companies to use this chapter to take a fresh look at their policies, practices and products, to create a safer and more inclusive online space for everyone.

