ETSI TR 103 936 V1.1.1 (2024-01)

Cyber Security (CYBER);
Implementing Design practices to mitigate consumer IoT-enabled coercive control

Reference
DTR/CYBER-0096

Keywords
IoT, security, user

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
https://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our
Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.
The content of the PDF version shall not be modified without the written authorization of ETSI.
The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document is an informative ETSI Technical Report (TR) that recommends initial design practices to minimize the potential of coercive control through the use of consumer Internet of Things (IoT) devices. The diversity and proliferation of consumer IoT devices provides new mechanisms that attackers might misuse, and this is a risk that should be addressed by industry.

The present document provides emerging design practices through examples and explanatory text for organizations involved in the development and manufacturing of Consumer IoT devices and associated services. The intent of the present document is to identify design practices to minimize potential misuse of Consumer IoT devices and associated services for coercive control whilst not limiting the intended functionality of the device by the user. Although the present document is focused on design practices for Consumer IoT devices, the guidance also applies to multiple other types of smart technologies including but not limited to Smart TVs, alarm systems, stereos, etc. The present document also covers the surrounding eco-system around consumer IoT devices, this includes how related technology, services, and the user behaviour of consumer IoT devices relates to the issues of coercive control.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Presentation to TC CYBER, ETSI; Jo Walker, Applied Research, BT; 29/09/2022: "Technology Enabled Coercive Control".

[i.2] ETSI TR 103 621 (V1.2.1): "Guide to Cyber Security for Consumer Internet of Things".

[i.3] UK Parliament: "Online Safety Bill".

[i.4] COM(2020) 825 final: "Proposal for a Regulation Of The European Parliament And Of The Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC".

[i.5] Austalian Government: "Online Safety Act 2021".

[i.6] LOI n 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet (LAW n 2022-300 of March 2nd, 2022 aimed at strengthening parental control over the means of access to the Internet).

[i.7] Bulletin of the New York Academy of Medicine: "Communist Attempts to Elicit False Confessions from Air Force Prisoners of War", vol. 33, no. 9, Sept. 1957, pp. 616-25; Biderman, Albert D.

[i.8] Kenneth Pettersen Gould & Corinne Bieder: "The Coupling of Safety and Security", 22nd August 2020, Safety and Security: The Challenges of Bringing Them Together, pp. 1-8.

[i.9] Maitreayee Bora: "The ultimate guide to design for safety", December 20th 2021.

[i.10] IBM: "Five Technology Design Principles to Combat Domestic Abuse", November 11th 2020.

[i.11] Jane Murison: "Trauma Informed Design", October 21st 2021.

[i.12] Eric Zeng, Shrirang Mare, and Franziska Roesner: "End User Security and Privacy Concerns with Smart Homes", July 12-14, 2017, University of Washington.

[i.13] Janet X. Chen, Allison McDonald, Yixin Zou, Emily Tseng, Kevin Roundy, Acar Tamersoy, Florian Schaub, Thomas Ristenpart, and Nicola Dell: "Trauma-Informed Computing: Towards Safer Technology Experiences for All", April 29-May 5, 2022.

[i.14] COM(2022) 105 final: "Proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence".

[i.15] FCC: "FCC Looks to Help Domestic Violence Survivors Access Connectivity", 17th February 2023.

[i.16] Samsung Mobile Press: "Evolving for the Better: SmartThings Ecosystem Gives Galaxy Users Better Control Over Their Connected Devices", April 20th 2021.

[i.17] ETSI EN 303 645 (V2.2.2): "CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements".

[i.18] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. "'A Stalker's Paradise': How intimate partner abusers exploit technology". In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems. ACM, 2018, doi: 10.1145/3173574.3174241.

[i.19] D. Cikanavicius: "Gaslighting: What It Is and Why It's So Destructive", 2nd October 2017.

[i.20] Parliament of Australia, Inquiry into Family, Domestic and Sexual Violence, Section 4: "Non-physical forms of violence".

[i.21] Yardley, Elizabeth: "Technology-Facilitated Domestic Abuse in Political Economy: A New Theoretical Framework", Violence Against Women, vol. 27, no. 10, Aug. 2021, pp. 1479-98, doi: 10.1177/1077801220947172.

[i.22] Havron, Sam, Freed, Diana, Chatterjee, Rahul, McCoy, Damon, Dell, Nicola, Ristenpart, Thomas: "Clinical Computer Security for Victims of Intimate Partner Violence", Proceedings of the 28th USENIX Security Symposium, 2019.

[i.23] Callaghan, Jane E. M., et al.: "Beyond 'Witnessing': Children's Experiences of Coercive Control in Domestic Violence and Abuse", Journal of Interpersonal Violence, vol. 33, no. 10, May 2018, pp. 1551-81.

[i.24] Katz, Emma. "Beyond the Physical Incident Model: How Children Living with Domestic Violence Are Harmed By and Resist Regimes of Coercive Control: Children's Experiences of Coercive Control", Child Abuse Review, vol. 25, no. 1, 2016, pp. 46-59.

[i.25] Katz, Emma: "When Coercive Control Continues to Harm Children: Post-Separation Fathering, Stalking and Domestic Violence", Child Abuse Review - Wiley Online Library, 2020 doi: full/10.1002/car.2611.

[i.26] Stark, Evan: "Coercive Control: How Men Entrap Women in Personal Life". Oxford University Press, 2007.

[i.27] Nikupeteri, Anna, et al.: "Coercive Control and Technology-Facilitated Parental Stalking in Children's and Young People's Lives", Journal of Gender-Based Violence, vol. 5, no. 3, 2021, pp. 395-412.

[i.28] Dragiewicz, Molly, et al.: "'What's Mum's Password?': Australian Mothers' Perceptions of Children's Involvement in Technology-Facilitated Coercive Control", Journal of Family Violence, vol. 37, no. 1, Jan. 2022, pp. 137-49, doi: 10.1007/s10896-021-00283-4.

[i.29] Yixin Zou and Allison McDonald, Julia Narakornpichit, Nicola Dell and Thomas Ristenpart, Kevin Roundy, Florian Schaub, Acar Tamersoy: "The Role of Computer Security Customer Support in Helping Survivors of Intimate Partner Violence", Proceedings of the 30th USENIX Security Symposium.

[i.30] ETSI TR 102 202 (V1.1.2): "Human Factors (HF); Human Factors of work in call centres".

[i.31] ETSI TR 102 133 (V1.1.1): "Human Factors (HF); Access to ICT by young people: issues and guidelines".

[i.32] ETSI TR 103 073 (V1.1.1): "Universal Communications Identifier (UCI); Improving communications for disabled, young and elderly people".

[i.33] ETSI EG 202 301 (V1.1.1): "Universal Communications Identifier (UCI); Using UCI to enhance communications for disabled, young and elderly people".

[i.34] ETSI EG 202 423 (V1.1.1): "Human Factors (HF); Guidelines for the design and deployment of ICT products and services used by children".

[i.35] ETSI EG 202 745 (V1.1.1): "Human Factors (HF); Guidelines on the provision of ICT services to young children".

[i.36] UK Parliament: "Technology and domestic abuse", 13th November 2020.

[i.37] Havard, Elizabeth Tirion: "Beyond proximity : the covert role of mobile phones in maintaining power and coercive control in the domestic abuse of women", PhD Thesis, University of Sussex, ISNI 0000 0004 8503 2422, 2019.

[i.38] Julia Slupska, Angelika Strohmayer: "Networks of Care: Tech Abuse Advocates' Digital Security Practices", Proceedings of the 31st USENIX Security Symposium, August 2022.

[i.39] Madison Lo: "A Domestic Violence Dystopia: Abuse via the Internet of Things and Remedies Under Current Law", Note Volume 109; February 2021.

[i.40] World Health Organisation (WHO): "Violence against women", 2013 [accessed 21st July 2023].

[i.41] World Health Organisation (WHO): "Violence Against Women Prevalence Estimates, 2018", [accessed 21st July 2023].

[i.42] IHS Markit: "The Internet of Things: a movement not a market", [accessed 21st July 2023].

[i.43] Domestic Abuse Act 2021.

[i.44] Dobash, R.P., Dobash, R.E., Wilson. M. and Daly. M.: "The myth of sexual symmetry in marital violence", Social Problems, 39(1), pp. 71-91, 1992.

[i.45] Johnson, M. P.: "Conflict and Control: Gender Symmetry and Asymmetry in Domestic Violence", Violence Against Women, 12(11), pp. 1003-18, 2006, doi: 10.1177/1077801206293328.

[i.46] Mennicke, A. and Kulkarni, S.: "Understanding Gender Symmetry within an Expanded Partner Violence Typology", Journal of Family Violence, 31(8), pp. 1013-1018, 2016, doi: 10.1007/s10896-016-9867-2.

[i.47] Stark, E.: "Do violent acts equal abuse? Resolving the gender parity/asymmetry dilemma", Sex Roles, 62(3-4), pp. 201-211, 2010, doi: 10.1007/s11199-009-9717-2.

[i.48] Pence E. & Paymar M.: "Education groups for men who batter: the Duluth model". New York, Springer publishing company, 1993.

[i.49] Cook, S. L. and Goodman, L. A. "Beyond Frequency and Severity: Development and Validation of the Brief Coercion and Conflict Scales", Violence Against Women, 12(11), pp. 1050-1072, 2006, doi: 10.1177/1077801206293333.

[i.50] Arnold, G.: "A battered women's movement perspective of Coercive Control", Violence Against Women, 15(12), pp. 1432-1443, 2009, doi: 10.1177/1077801209346836.

[i.51] Harne, L. and Radford, J.: "Tackling domestic violence, theories, policies and practice. Berkshire", Open University Press, 2010.

[i.52] Ali, P. A. and Naylor, P. B.: "Intimate partner violence: A narrative review of the feminist, social and ecological explanations for its causation", Aggression and Violent Behavior, 18(6), pp. 611-619, 2013, doi: 10.1016/j.avb.2013.07.009.

[i.53] Warford, N., Matthews, T., Yang, K., Akgul, O., Consolvo, S., Kelley, P. G., Malkin, N., Mazurek, M. L., Sleeper, M., Thomas, K.: "SoK: A Framework for Unifying At-Risk User Research", 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2022, pp. 2344-2360, doi: 10.1109/SP46214.2022.9833643.

[i.54] Elliott, A. and Brody, S.: "Straight talk: New Yorkers on mobile messaging and implications for privacy", Technical report, Simply Secure, 2015.

[i.55] Karla Badillo-Urquiola, Xinru Page, and Pamela J. Wisniewski.: "Risk vs. restriction: The tension between providing a sense of normalcy and keeping foster teens safe online". In Proc. CHI, 2019.

[i.56] Arup Kumar Ghosh, Karla Badillo-Urquiola, Shion Guha, Joseph J. LaViola Jr, and Pamela J. Wisniewski.: "Safety vs. surveillance: What children have to say about mobile apps for parental control". In Proc. CHI, 2018.

[i.57] Tara Matthews, Kerwell Liao, Anna Turner, Marianne Berkovich, Robert Reeder, and Sunny Consolvo. "'She'll just grab any device that's closer': A Study of Everyday Device & Account Sharing in Households". In Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems (CHI '16), 2016 doi: 10.1145/2858036.2858051.

[i.58] Clara Berridge, Jodi Halpern, and Karen Levy.: "Cameras on beds: The ethics of surveillance in nursing home rooms". AJOB Empirical Bioethics, 10(1):55-62, 2019.

[i.59] Sofie Kodner: "How new monitoring systems keep a close watch on older people", The Washington Post.

[i.60] Clara Berridge, MSW, PhD, Terrie Fox Wetle, MS, PhD: "Why Older Adults and Their Children Disagree About In-Home Surveillance Technology, Sensors, and Tracking", The Gerontologist, Volume 60, Issue 5, August 2020, Pages 926-934, doi: 10.1093/geront/gnz068.

[i.61] Jordan Hayes, Smirity Kaushik, Charlotte Emily Price, and Yang Wang: "Cooperative privacy and security: Learning from people with visual impairments and their allies". In Proc. SOUPS, 2019.

[i.62] Tousif Ahmed, Roberto Hoyle, Kay Connelly, David Crandall, and Apu Kapadia: "Privacy concerns and behaviors of people with visual impairments". In Proc. CHI, 2015.

[i.63] Manya Sleeper, Tara Matthews, Kathleen O'Leary, Anna Turner, Jill Palzkill Woelfer, Martin Shelton, Andrew Oplinger, Andreas Schou, and Sunny Consolvo: "Tough times at transitional homeless shelters: Considering the impact of financial insecurity on digital security and privacy". In Proc. CHI, 2019.

[i.64] Kurt Thomas, Patrick Gage Kelley, Sunny Consolvo, Patrawat Samermit, and Elie Bursztein: "'It's common and a part of being a content creator': Understanding How Creators Experience and Cope with Hate and Harassment Online". In Proceedings of CHI 2022. Article 121, 1-15, doi: 10.1145/3491102.3501879.

[i.65] Morgan Klaus Scheuerman, Jialun Aaron Jiang, Casey Fiesler, and Jed R. Brubaker: "A Framework of Severity for Harmful Content Online". Proc. ACM Hum.-Comput. Interact. 5, CSCW2, Article 368 (October 2021), 33 pages, 2021, doi: 10.1145/3479512.

[i.66] Rosie Bellini, Emily Tseng, Noel Warford, Alla Dafalla, Tara Matthews, Sunny Consolvo, Jill Palzkill Woelfer, Patrick Gage Kelley, Michelle L. Mazurek, Dana Cuomo, Nicola Dell, Thomas Ristenpart: "SoK: Safer Digital-Safety Research Involving At-Risk Users", IEEE Symposium on Security and Privacy, 2024, To appear.

[i.67] ETSI TS 103 643 (V1.2.1): "Techniques for assurance of digital material used in legal proceedings Assuring digital material".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

attacker: anyone who introduces digital-safety assault or harms to another person, regardless of the severity or intention (i.e. attackers may intentionally or unintentionally cause harm)

NOTE: This could include a broad range of individuals or groups, a family member, a stranger, or a nation-state.

coercive control: act or a pattern of abusive acts (such as physical assault, security breach, privacy invasions, harassment, etc.) that results in limited autonomy and/or emotional harm to a potential target, whether or not such abuse or harm was the intent

consumer IoT device: network-connected (and network-connectable) device that has relationships to associated services and are used by the consumer typically in the home or as an electronic wearable

NOTE: As defined in [i.17].

consumer IoT-enabled abuse: controlling and coercive behaviours using Consumer IoT products

controlling behaviour: range of acts designed to make a person subordinate and/or dependent by isolating them from sources of support, exploiting their resources and capacities for personal gain, depriving them of the means needed for independence, resistance and escape and regulating their everyday behaviour

gaslighting: form of psychological manipulation in which a person seeks to sow seeds of doubt in a targeted individual or in members of a targeted group, making them question their own memory, perception, or sanity

product: device or service provided by a manufacturer or service provider

target, or targeted user: person who is the target of an attacker, digital-safety attacks, IoT-enabled abuse, or coercive control

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

CCTV	Close-Circuit TeleVision
DARVO	Deny Attack Reverse Victim and Offender
DDoS	Distributed Denial-of-Service
EG	ETSI Guide
GDPR	General Data Protection Regulation
GPS	Global Positioning System
GSMA	Global System for Mobile communications Association
HF	Human Factors
ICT	Information and Communication Technology
IoT	Internet of Things
IPA	Intimate Partner Abuse
NGO	Non-Government Organisation
TC	Technical Committee
TFA	Technology Facilitated Abuse
TV	TeleVision
UCI	Unified Configuration Interface
UI/UX	User Interface design / User eXperience design
UN	United Nations

WHO World Health Organization

4 Background Information

4.1 Introduction

The present document provides general guidance to ETSI and Consumer IoT product providers on the best design practices to mitigate against Consumer IoT-enabled coercive control. The present document builds upon previous work conducted in ETSI TC Cyber (see clause 5 of ETSI TR 103 621 [i.2] which briefly discusses how Consumer IoT devices can be misused against vulnerable cohorts).

While Consumer IoT has brought considerable social benefits, some individuals intend to use them for harm. Some targets and attackers may be strangers to each other. However, generally a personal connection with each other through a family, friend, acquaintance, professional relationship, or intimate relationship is fair more common. While a substantial body of studies have documented coercive control involving intimate relationships, e.g. [i.18], [i.21], [i.22], [i.26], [i.29], [i.37], safety concerns related to coercive control can arise in a variety of other relationship contexts. It is these latter relationships - and the potential for harm that emerges in this context - that are the focus of the present document. For example, children are often subject to parental monitoring and control of their technology use, and these activities can range from reasonable precautions to privacy invasions and abuse [i.55], [i.56]. Older adults who rely on caregivers may reluctantly forfeit privacy for physical safety or the ability to live at home [i.58], [i.59], [i.60]. People with visual impairments may rely on others to help with technology, opening them up to privacy invasions [i.61], [i.62]. People who are financially insecure may stay on family mobile plans with untrusted family members because they cannot afford separate service, opening them up to unwanted surveillance [i.54], [i.63]. Roommates may share technology in their shared home, and be subject to privacy invasions, pranks, or security concerns [i.57]. While many of these examples could involve healthy, trusting relationships, not all do, and even typically trustworthy relations can violate safety expectations. Any of these groups - and more who have relationship risk factors, as covered in [i.53] - may be more susceptible to coercive control abuses via technology in bounded moments or over time. These diverse groups and scenarios suggest a wide range of contexts that may be relevant to Consumer IoT product providers aiming to help protect users from coercive control.

Everyday Consumer IoT products that are, for the most part, taken for granted within personal relationships can be repurposed for coercive control. This coercive control creates trauma, both when it is being experienced, and in its aftermath. It is imperative that organizations involved in creating Consumer IoT products understand the potential ramifications of their products and services, raise awareness and adopt authentic trauma-informed approaches to their business practices. As such, the present document presents guidance in the two related spheres of coercive control resistant design and trauma informed practice.

The present document intends to help IoT product providers identify the actions required to be aligned with upcoming, stricter EU legislation to mitigate potential consumer IoT- enabled abuse. Below is a non-exhaustive list of recently passed and upcoming legislative acts.

These include a non-exhaustive list:

1) UK Online Safety Bill, intended to improve internet safety [i.3].

2) EU Digital Services Act [i.4], to modernize the e-Commerce Directive regarding illegal content, transparent advertising, and disinformation.

3) Australian Online Safety Act 2021 [i.5] expands protections against online harm, to keep pace with abusive behaviour and toxic content.

4) France's Law LOI n 2022-300 du 2 mars 2022 visant à renforcer le contrôle parental sur les moyens d'accès à internet (LAW n 2022-300 of March 2nd, 2022 aimed at strengthening parental control over the means of access to the Internet) [i.6].

5) Directive of the European Parliament and of the council on combating violence against women and domestic violence [i.14].

6) USA Federal Communications Commission, Proposed rule on Supporting Survivors of Domestic and Sexual Violence, Lifeline and Link Up Reform and Modernization, Affordable Connectivity Program [i.15].

The broader focus of the present document on Consumer IoT enabled coercive control is to expose potential risks associated with coercive control abuse from the misuse of Consumer IoT products. The design solutions and recommended best practices in this complex problem space are largely unknown at this time and will require future research to develop [i.8].

While the present document focuses on Consumer IoT some of the design principles discussed could equally be applied to other areas such as Industrial IoT, and eHealth, pending new investigations and research. However, there are some limitations to applying the design principles as coercive control is not just a security and privacy design issue. Coercive control often builds on existing relationships (e.g. caretaker, partner, parent) and abusing the power dynamics within that relationship. An example of that Industrial IoT and eHealth could apply design principles about privacy to minimize risks that could further coercive control, e.g. limiting access to sensitive health data from employees and processes to prevent unauthorised parties from gaining access. Also, the use and functionality of industrial IoT may require functions for safety which could be considered intrusive in a consumer environment. Similarly for a medical device used in an eHealth domain, the device has to be certified specifically for medical use, that includes tests not often applied to consumer devices. There is a separate area of research for the topic of workplace coercive coercion that the present document does not cover. While the present document addresses consumer IoT other sectors can take the recommendations presented here into account if they so choose.

By raising awareness of the ways Consumer IoT Products can be used for coercive control, the present document takes a first step toward seeking mitigations for the safety issues outlined in future research.

4.2 Emerging concern about Consumer IoT Enabled Coercive Control

The concerns that have been raised about the misuse of novel telecommunications applications such as smartphones, tablets, social media, wearables, smart speakers, telecare systems, internet connected cars, internet connected home appliances, smart locks, smart thermostats, and home security systems in the context of coercive control within intimate relationships often known as Consumer IoT Enabled abuses or Technology Facilitated Abuse (TFA) [i.1]. TFA behaviours include but are not limited to stalking and omnipresence, surveillance (wiretapping, bugging, videotaping, geolocation tracking, data mining, social media mapping, and the monitoring of data and traffic on the internet), intimidation, impersonation, humiliation, threats, consistent harassment/unwanted contact, sexting, and image-based sexual abuse.

It can also be referred to by various names including Consumer IoT enabled facilitated domestic abuse, digital dating abuse, Consumer IoT enabled coercive control, digital coercive control, Consumer IoT enabled misuse.

NOTE 1: See bibliography for additional references.

Coercive control is entrapment in personal life, and it pertains to the set of control skills also used in other situations of captivity such as hostage situations and human trafficking to override autonomy and the sense of self and entrap a person. Coercive control in the context of domestic abuse entraps a person (mainly women) in personal life excluding them from meaningful participation in wider society. Coercive control does not refer to mutually antagonistic couples, conflict consisting of sporadic incidents of abuse or violence.

NOTE 2: See bibliography for additional references.

4.3 Understanding Tech Abuse

4.3.1 Introduction

Coercive control is a type of abuse that tends to occur in the context of interpersonal relationships. Prior work by Warford et al. [i.53] developed a framework of relationship risk factors, which helps organizations understand the user groups that may face relationship-based risks and the kinds of attacks and harms they experience. To identify risk factors, Warford et al. performed an analysis on 95 peer-reviewed papers published in computer security and human-computer interaction venues on digital safety and at-risk users, i.e. users who experience temporary or ongoing contextual risk factors that elevate the chance of digital attacks or harm from such attacks. Three relationship risk factors were identified from their review:

1) Having a relationship with the attacker: A personal relationship with an untrustworthy person may put a person at risk of attacks that take advantage of personal knowledge of them, physical access to them or their devices, or relational power dynamics. From the review, this included populations such as survivors of IPA, foster teens, older adults, women in repressive regions, people who were financially insecure, crowd workers, and survivors of trafficking.

2) Having a reliance on a third party: By providing needed or safety-focused help or care, a third party can (often inadvertently) contribute to risks of privacy invasions from the third party, an increased attack surface through the third-party, or an attacker impersonating the third party. From the review, this included populations such as children, teens, foster teens, older adults, people with visual impairments, women in repressive regions, refugees, survivors of sexual assault, survivors of IPA, and survivors of trafficking.

3) Having access to other at-risk users: Having access to at-risk users can make the individual with that access become at-risk themselves, as it increases risk of a range of stepping-stone attacks aimed to access or harm the other at-risk users. From the review, this included populations such as people involved with U.S. political campaigns, teachers, journalists, and NGO staff.

Collectively, research papers that identify relationship risks describe safety issues people are concerned about or have experienced in their interpersonal relationships. More serious safety issues can arise in any of these contexts where trust breaks down or the health of the relationship falters, something that can occur in short periods of conflict or due to other life circumstances.

Warford el al. [i.53] also describe seven non-relationship risk factors that can create intersectional risk and change how people experience relationship risks - these include legal or political factors, marginalization, social norms, prominence, resource or time constraints, underserved accessibility needs, and access to sensitive resources. When thinking through how to support people experiencing relationship risks, policy makers and Consumer IoT product providers should consider how a variety of risk factors - individually or in combination - may impact their user base. For example, people who are financially insecure may need to share devices or technology service plans with untrustworthy family members, opening them up to surveillance [i.54], [i.63]. Their resource constraints risk factor interacts with having a relationship with their attacker, to create these threat scenarios. As another example, older adults with disabilities may be surveilled by family members to ensure their safety (the reliance on a third-party risk factor) [i.58], though their disabilities may hinder their ability to understand or control this surveillance (the underserved accessibility needs risk factor).

4.3.2 Example: Intimate partner abuse

A common example of coercive control via technology is in the context of intimate partner abuse, which often involves violence against women. Violence (physical, sexual, or psychological) by a husband or male intimate partner is the most widespread form of violence against women globally [i.40], [i.41]. It is estimated that almost one third (30 %) of women who have been in a relationship have experienced sexual and/or physical violence with 38 % of female homicides committed by intimate partners [i.40], [i.41]. The 2030 United Nations (UN) Agenda for Sustainable Development Goals identified the need to achieve gender equality and empower all women and girls. The global target is to eliminate *"all forms of violence against women and girls in the public and private spheres"* [i.41].

There has also been an unprecedented global dependence on and development of technology. Internet connected 'smart' technologies are increasingly part of our everyday lives and include, but are not limited to smart phones, laptops, tablets, smartwatches, home assistants and home security systems. These technologies are often referred to as "The Internet of Things" (IoT). Whilst it is difficult to predict the growth of the IoT, it is estimated that the number of IoTs will reach 125 billion by 2023. IoT represents a constantly evolving movement of profound change in how humans interact with machines, information, and each other [i.42]. Whilst IoT devices offer many potential benefits, there is no doubt that they also offer opportunities to facilitate and enhance intimate partner abuse.

While intimate partner abuse is not the only way Consumer IoT technologies can be used for coercive control, it is an important class of abuse for IoT product providers to be aware of. Emphasizing this kind of abuse aligns with the UN's call for the elimination of violence by considering the role of technology in the abuse, coercion, and control of women by current/former partners and family members.

The importance of women's experience to the present documentreflects current understanding and established research [i.43], [i.44], [i.45], [i.46], [i.47] that abuse within intimate/familial relationships is gender asymmetric, i.e. abuse is predominantly perpetrated by men against women. However, the present document does not, in any way, deny that abuse happens from women to men or within same sex relationships. Indeed, it is anticipated that much of what is considered within the present document is applicable to survivors of intimate partner abuse regardless of age, disability, race, religion/belief, sex, gender, or sexual orientation. Nor does the present documentconsider intimate partner abuse the only way Consumer IoT devices may be misused for coercive control.

4.4 Types of Consumer IoT enabled Abuse

There are many different ways an attacker may use Consumer IoT systems to facilitate coercive control. Thomas et al. [i.64] developed a taxonomy of online hate and harassment attacks, which can help consumer IoT product providers and policy developers understand the broad range of tactics attackers may employ to target various user groups. This taxonomy was developed from an extensive literature review (of 150 research papers and prominent news stories) and 3-year survey of 50 000 participants globally with a range of demographics and experiences. It includes seven categories of online attacks:

- Toxic content covers a wide range of attacks involving media that attackers send to a target or audience - e.g. bullying, trolling, threats of violence, and sexual harassment - which can result in emotional harm and marginalization (as targets may avoid engaging online to escape these attacks).
- Content leakage involves any scenario where an attacker leaks (or threatens to leak) sensitive, private information to a wider audience, typically with the intent to embarrass, threaten, intimidate, or punish the target.
- Overloading includes any scenario wherein an attacker forces a target to triage myriad notifications or comments via amplification, or otherwise makes it technically infeasible for the target to participate online due to jamming a channel (potentially via a DDoS attack).
- False reporting broadly captures scenarios where an attacker deceives a reporting system or emergency service - originally intended to protect people - to falsely accuse a target of abusive behaviour.
- Impersonation occurs when an attacker relies on deception of an audience to assume the online persona of a target in order to create content that will damage the target's reputation or inflict emotional harm.
- Surveillance involves an attacker leveraging privileged access to a target's devices or accounts to monitor the target's activities, location, or communication.
- Lockout and control involves scenarios where an attacker leverages privileged access to a target's account or device - including computers, or Consumer IoT devices - to gaslight the target or interfere with how they engage with the world.

Attacks like these often cause substantial harm. Scheuerman et al. [i.65] developed a framework of severity for harmful content online, including four types of harm and eight dimensions along which severity of harm can be understood. This framework can help IoT product providers and policy developers assess what harms may be caused by Consumer IoT devices and whether mitigations have been employed to lessen their severity. The types of harm in the framework are:

- Physical harm is bodily injury to an individual or group of individuals, including self-injury, sexual abuse, or death.

- Emotional harm ranges from an annoyance (at its least severe) to a stressful or traumatic emotional response (at its most severe), whether fleeting or long-lasting.
- Relational harm is defined as damage to one's reputation or their interpersonal, professional, or larger community relationships.
- Financial harm is defined as material or financial loss, including the loss of digital assets (like accounts) and the loss of economic opportunity (such as job loss or disqualification from employment).

Some additional examples of Consumer IoT abuse tactics and harms are outlined in table 1.

Table 1: Consumer IoT abuse tactics and harms [i.7]

Coercion tactic	Purpose	Tech Abuse Example
Isolation	Isolation is a tactic used to deprive the target of social support. When a target is isolated, they have no one to turn to for help. This makes it harder for them to leave the abusive relationship or to resist the attacker's demands. This also isolates the target from alternative perspectives about problems in their relationship that family/friends may flag. By isolating the target, the attacker makes the target more dependent on them for everything. This may include emotional support, financial support, and even transportation. This makes it more difficult for the target to leave the abusive relationship as they are not sure how they will cope without these supports. Allows the attacker to discredit the target to others. When a target is isolated from people in their life, the attacker often becomes the liaison between the target and the outside world. This makes it difficult for the target to defend themselves or their actions as they are not allowed to communicate with others.	Monitoring the target's online activity. Attackers can use tracking software to see what websites the target visits, who they email, and what they post on social media. This allows the attacker to control the target's online life and isolates the target by preventing them from communicating with others. Stealing the target's devices or deleting their online accounts. Attackers may steal the target's device so that they can control their access to technology or delete their online accounts. This can make it difficult for the target to stay in touch with friends and family, and it can prevent them from seeking help. Misusing of smart locks to restrict movements. Attackers can use smart door locks to trap targets inside a house or control/monitor who comes and goes. This, in turn, will further isolate the target from others and imprison the target from seeking physical help. Sharing biased information online. Compromising information used to misrepresent or humiliate a person to others, e.g. image-based abuse or social media smear campaigns. Attackers create a positive image of themselves and their relationship on social media to ensure the target is disbelieved, should they disclose the abuse.

Coercion tactic	Purpose	Tech Abuse Example
Monopolization of perception	Attackers tend to use monopolization perception techniques to isolate the target from their friends and family. This makes it difficult for the target to recognize that abuse is taking place, to get a second opinion or to have someone to talk to who is not under the attacker's control. Attackers also use monopolization techniques to make the target feel like they are crazy or imagining things. This makes the target doubt their own judgment and makes them more likely to believe the attacker. Perspective of the attacker becomes the only acceptable narrative even when completely at odds with reality. Monopolization of perception techniques may also be used to make the target feel they are dependent on the attacker and do not have any choice but to stay in their current situation. The attacker may use monopolization techniques to pose as morally superior to their target.	Using Consumer IoT devices, the attacker may control what information the target has access to on their phone. This can include limiting their access to news, social media, or other forms of communication. This can make it difficult for the target to get help or to learn about their rights. Using social media to control the target's online presence. Attackers can use social media to post embarrassing or hurtful messages about the target, or to spread lies and rumours about them. This can make the target feel like they are being publicly shamed and that they cannot escape the attacker's control. Manipulation of an IoT system and proliferation of compromising information used to gaslight the target and undermine the target's perceptions.
Monitoring	Monitoring is a tactic used by an attacker to track a target's activities and to ensure that they are not doing anything that the attacker disapproves of. Monitoring can be used to manipulate a target and remove their autonomy. If a target knows that their actions are being tracked, then they know that there may be repercussions if they act in a way that the attacker dislikes, hence they alter their behaviour and decisions. Constant monitoring instils anxiety within the target and can be used to intimidate the target. It can also be used to ensure a target does not seek help or support as they know that the attacker will know who they speak to and what they say.	Using social media to track who an attacker is "friends" with, who they communicate with and what they post. Using surveillance cameras within the house to monitor what the attacker does every day and also track who comes and goes from the household. Using Spyware to track emails, text messages and phone calls on the target's phone. Also using other tracking software to monitor the target's online activity. This allows the attacker to see what websites the target visits, who they email and text, and what they post on social media. This can make the target feel like they are constantly being watched and that they cannot do anything without the attacker knowing about it. Using smart-tags or tracking apps to track a target in real-time.

Coercion tactic	Purpose	Tech Abuse Example
Threats	Threats are used by attackers to make them feel like they have some level of control over the target. Threats can be used to control how the target behaves and speaks. Targets often feel like they have to comply with the attackers wishes or else the threats may become a reality. Constant threats from the attacker cultivates anxiety and despair within the target. It makes them feel like they always have to be on guard. Hence, are unable to relax or feel comfortable in their environment. This often causes both mental and physical repercussions to the target. Promotes dissociation and autonomic responses that reduce personal agency and can be manipulated to portray the target as crazy or unstable.	Attackers may threaten to expose compromising photos or videos of a target if they refuse to comply with the attackers demands. This may in the form of image-based abuse or revenge pornography. Attackers may have access to the target's social media accounts and may threaten to send hateful messages to family/friends to damage the target's reputation and relationships with others. Attackers can also threaten to remove or limit a target's access to Consumer IoT devices that they may depend on within their ecosystem for example, accessing the controls on the smart thermostats, smart door locks, smart TVs, etc.
Degradation	Degradation is a tactic used to belittle the target and make them feel worthless. It can make them feel like they are not worthy of respect or dignity. This can make it difficult for the target to stand up for themselves or seek help. It also allows the attacker to implement "breadcrumbing", an act that keeps the target hopeful that the attacker has changed - but not enough to make them feel comfortable or assured the relationship is going well. The attacker can emotionally manipulate the target this way. Degradation can be used to make the target feel guilty or responsible for the attacker's behaviour. This can make it difficult for the target to know that they are being abused and it can also make it harder for them to leave the attacker. Degradation tactics can be used to intimidate the target and make them feel powerless and scared. This makes it difficult for the target to stand up for themselves and resist the attackers demands. It can make the cost of resistance appear more damaging to self-esteem than capitulation. Degradation can have a major impact on a target's mental and emotional health. Degradation tactics can make it difficult for targets to trust people and form healthy relationships.	Attackers can taunt targets with a proliferation of compromising information that can be used to degrade, such as image-based abuse. Consumer IoT devices like smartphones, smartwatches, smart TVs can be used as weapons to facilitate this abuse. Attacks can also degrade a target by withholding use of Consumer-IoT resources, e.g. control of a smart thermostat to maintain adequate heating or use of smart appliances such as smart speakers to turn off music. Attacks can also degrade the target by restricting their movements by either locking them inside or outside of the house using smart door locks, or by using security cameras to monitor their movements.

Coercion tactic	Purpose	Tech Abuse Example
Occasional indulgences	Occasional indulgences from the attacker provides positive motivation for compliance. It makes the target think that if they obey the attacker's demands all of the time, they will not suffer from abuse. Occasional indulgences can also create confusion over the attacker's true-nature. It makes the target doubt if they are really being abused or about the extent of the abuse in the past. It can induce guilt over aggressive feelings towards the attacker and can pull the target back into mean-sweet abuse cycles. This in turn makes it harder for the target to leave.	The attacker may gift the target with a consumer-IoT device and may even help them set it up. Although this seems like a kind gesture, by allowing them to set up the device they may gain access to the devices passwords and settings which may later be used against the target. An attacker may use social media to praise a target which makes the target feel worthy, loved and seen for a short period of time. The intermittent good treatment by the attacker creates trauma bonding and makes it difficult for the target to leave or escape their attacker.
Deny Attack Reverse Victim and Offender (DARVO)	DARVO is used by attackers to deny any wrongdoing or abuse, and instead attack the target for attempting to hold the attacker accountable for their actions. The attacker then claims that they are the victim and that the person who was abused is actually the perpetrator. DARVO can make the target feel confused and disoriented. It can make them question if they were abused at all and reluctant to speak to others in case they are the perpetrators. DARVO can also make the target feel guilty if they believe what the attacker is telling them. This makes them try to please the attacker even more and makes them more reluctant to seek any external advice.	Attackers may delete any evidence of abuse that may be stored on Consumer-IoT devices. In the absence of hard evidence, the target is forced to rely on their own memory which can be manipulated by the attacker.
Induced debility and exhaustion	Induced debility and exhaustion weakens the target's mental and physical ability to resist abuse as they feel drained.	An attacker can harass the target with repeated phone calls and constant demands creating a sense that there is no respite from demands of the attacker. The attacker could also use a smart speaker or smart music device to blare music at random times during the night which would prevent the target from sleeping and would also make them feel very uneasy, anticipating the next sound.

5 Designing for Safety

5.1 Introduction

Safety is both a feeling and a reality, and they are different. An individual might feel safe even though they are not, and they might be safe even if they do not feel safe.

The present document seeks to recommend design practices that are built around the target. A crucial element of this is the continued empowerment of the target. Targets of Consumer IoT enabled abuse often have encountered multiple systems, in which well-meaning professionals have encouraged them to pursue a particular course of action. However, this can serve to create a new locus of control, where the power that was concentrated in the hands of the attacker transfers to another person.

NOTE: Additional guidance discussing safety from ETSI HF about Communications services, ICT products and services for children, disabled and the elderly:

- ETSI TR 102 133 [i.31]. It reviews the human interaction issues for access to ICT by children and provides guidance on how these should be dealt with. This will also include the ethical and legal issues of security for vulnerable children accessing public communications spaces.
- ETSI TR 103 073 [i.32]. It reports on the use of UCI systems to improve communications for disabled, young people (up to 12 years of age) and elderly people.
- ETSI EG 202 301 [i.33]. It presents recommendations that address the issues identified in ETSI TR 103 073 [i.32] which identified communications issues experienced by people with disabilities, elderly people, and young people up to 12 years of age.
- ETSI EG 202 423 [i.34]. it provides guidelines for standards developers and ICT designers on how to take account of the needs of children (12 years and younger) in the design and deployment of ICT products and services.
- ETSI EG 202 745 [i.35]. It provides guidelines for service and content providers who are deploying and provisioning ICT services that are being used, although not necessarily purchased, by young children less than 12 years of age.

5.2 Elements of Designing for Safety

5.2.1 Research

Every Consumer IoT product provider should perform research. However, abuse contexts involve elevated risk for users, so research with relevant participants should be approached with care. Teams should use the lowest risk research method that will address their research questions, typically starting with a literature review. Direct engagement with users experiencing coercive control should only be approached under the guidance of experts and with training - see [i.66] for more guidance. This design research should consist of a wide analysis of how exactly their Consumer IoT product may be leveraged for abuse as well as understanding the possible experiences of targets and attackers ideally by working or collaboration with organizations in this area. Researchers should investigate problems of interpersonal harm and abuse, exploring any other aspects of safety which may be a concern for the product or service, such as data security, biased algorithms, and harassment, etc. Abuse contexts involve elevated risk for users, research with these users should be approached with care. Teams should use the lowest risk research method that will address their research questions, typically starting with a literature review. It is important to note that there is no one-size-fits-all solution, and each abuse case may vary based on the scenario. Abusive situations tend to be ever-changing and require constant vigilance by targets, who best know their attacker and how to protect themselves.

5.2.2 Archetypes

After research, a product designer can use these insights to create attacker and target archetypes. Archetypes should not be based on actual individuals but instead a combination of research findings.

The attacker archetype looks at a product as a tool to perform harm or damage. Such attackers might try to cause harm to someone whom they do not know via surveillance or anonymous harassment, or may try to monitor, control, abuse, or harm someone whom they personally know. Additionally, individuals who takes control of a device in a potentially harmful way without intentionally meaning to cause harm to the target still falls into the attacker archetype [i.12].

The target archetype may experience Consumer IoT enabled Abuse. There are numerous situations to consider regarding the archetype's understanding of the abuse and how to stop it. For example, how do targets know that abuse is happening? How do they know the effects of the abuse? What actions can they take to prevent or ameliorate it? How might these actions put the target in danger?

Other types of archetypes could include "Situations" or "environmental factors". For example, the situations where privacy is restricted as in a refugee camp or a hospital. Additionally, there are certain factors that make it more likely that an attacker gets access for example low digital competence on the side of the target. Attackers might offer assistance to manage an IT problem and use this to implement a backdoor to gain access.

The product designer may want to create various target archetypes to capture a wide range of different experiences. The targets might know that the abuse is taking place but are unable to stop it, for example, an attacker may lock them out of IoT devices, which they are aware of but at the same time do not know how a stalker keeps tracking out their location. A designer can include as many scenarios as they want in their target archetype. These can be later used while designing solutions to allow their target archetypes to accomplish their goals of stopping and ending the abuse.

5.2.3 Designing Solutions

There are different methods that might help consumer IoT product providers design for safety [i.9].

Design of consumer IoT devices have implications across the technology stack, including among bodies that work on protocols and interoperability including IoT devices that do not have explicit UI/UX or user interaction through another company's software. It is preferable to have a list of known ways in which the product or service can be utilized for damage as well as attacker and target archetypes explaining opposing user goals. Then the next step is to recognize means or methods to design against the identified attacker's goals and to provide support to the target's goals. Below are examples of questions that can be asked to help prevent damage and provide support to the archetypes:

1) If someone were to use certain types of features or mitigations, could that lead to physical violence or make the situation worse (e.g. losing a place to stay or residence)?

2) Can the product be designed in a manner that the identified damage cannot occur in the first place? If not, then what kind of roadblocks can be put up to mitigate the damage?

3) Can the design help the target realize that abuse is taking place through the product or service?

4) Can the design help the target understand what they should do to end this problem?

5) Can the design identify any kinds of user activity which would indicate some form of damage or abuse? Is it possible that the product can help the user access support?

6) Does the design facilitate intentional or unintentional abuse or control (e.g. only allowing one system manager)?

7) How can the Consumer IoT product be designed to detect criminal behaviours perpetrated by the attacker?

8) Can the Consumer IoT product be programmed to detect specific usage patterns unique to the user, and detect when someone else is using the device?

5.2.4 Safety Testing

Safety testing of the designed product from the perspective of both archetypes: the person who weaponizes the product for harm and the target of the harm. Like any other type of product testing, it will rigorously test out the safety solutions to recognize gaps and correct them and validate that the designs will be able to provide safety to users. However, rhe present document does not recommend engaging directly with users who may be experiencing coercive control as part of product safety testing, due to the potential safety concerns; whether and how to engage such users is a topic for future guides.

Safety testing and usability testing using the archetypes carried out on the device and its associated services. It is important to note that testing for safety involves testing from the outlook of both a target and an attacker, on the other hand, if there are multiple target archetypes to capture multiple scenarios, safety testing will involve having to test from the outlook of each one.

Target archetype testing helps highlight how easy it can be for somebody to abuse the intended use of a product. It can take reference from the goals in the attacker archetype. Usability testing is not separate from creating safer Consumer IoT products: technology should be easy for targets to use to identify, prevent, and minimize the harm of abuse. Targets should also be able to safely use Consumer IoT for essential tasks.

Attacker archetype testing involves recognizing how to provide information and support to the target. For example, by opposing the attempt made by an attacker to stalk somebody also can satisfy the goal of the target archetype, i.e. not to be stalked, therefore, separate testing will not be required from the target's perspective.

6 Coercive Control-Resistant Design

6.1 Introduction

Coercive Control-Resistant Design can be defined as safeguarding or designing products with anti-abuse protections by default to minimize attackers' ability to use these tools to harm targets whilst not limiting the access to the device functionality by the intended user. Also, addressing feature extensions in IoT devices and services to allow the at-risk user to seek help without interference from the coercive party [i.10]. There are different factors that can inform coercive control-resistant design. These include but are not limited to:

1) Build consensus and awareness on the nature of the problem.
2) Identify dilemmas and build consensus on acceptable solutions.
3) Harm considerations "built in, not bolted on".
4) Minimize risks of harms arising.
5) Disrupt harms that have arisen.
6) Able to feed into the development of a diverse range of telecommunications products.
7) Diverse design team.
8) Privacy and Choice.
9) Combat Gaslighting.
10) Security and Data.
11) Technical Ability.

However, such design principles should be sensitive to the dynamics of coercive control. For example, restricting an attacker's digital access to a target can sometimes serve to escalate the behaviour, resulting in other types of abuse. Furthermore, encouraging targets to delete their online profiles can serve to compromise their freedoms and liberties in line with the goals of the attacker.

Ideally, the designers should draw upon existing research which represents the needs of targets because targets know their attackers best, in general this means the targets are the best placed person to judge the level of risk and danger which designers should enable to draw upon this expertise.

6.2 Omnipresence attacks & harms

Without the implementation of preventative strategies, the misuse of modern telecommunications applications could lead to a significant intensification in the level of oppression that attackers of coercive control are able to enact due to a concept termed "abuser omnipresence" whereby the attacker engages in micro-surveillance and micro-regulation of the target. It is noted for example how through the misuse of smartphones, attackers erect a system of control similar to Bentham's panopticon such that the attacker takes on an "omnipotent omnipresence" where the mobile phone acts as the attackers eyes and the target becomes trapped. This leads the target to become conditioned to act in a docile manner responding automatically to the attackers demands under the credible threat of punishment or physical violence [i.37]. The ability for attackers to establish omnipotent omnipresence is historically unprecedented and goes beyond the scope, nature, and severity of traditional formulations of coercive control [i.20]. The question for example of whether or not the IoT is a panopticon is often posed, but the domestic abuse situation demonstrates that even existing technology such as smartphones are now already easily repurposed in this way in the abusive relational system.

In situations of coercive control, surveillance using modern telecommunications applications is a reliable marker that distinguishes relationships characterized by "Widespread Violence" with high levels of all forms of abuse, from relationships that are better characterized as "unhealthy". In other words, surveillance behaviours such as installing spyware and tracking an individual via their mobile phone are reliable markers of dangerous relationships where individuals are at serious risk of psychological, emotional, and physical harm. The research from Elizabeth Yardley's "Technology-Facilitated Domestic Abuse in Political Economy: A New Theoretical Framework" [i.21] into the relationship between surveillance behaviours using modern telecommunications technologies and coercive control states that *"these surveillance behaviours are conceptualized as part of a coercive control process; in coercive control, attackers set the stage for violence by creating attachment, creating and exploiting vulnerabilities, and wearing down resistance, then, in the second stage, attackers issue demands coupled with expected consequences if the demands are not followed. The surveillance piece is used to monitor target compliance. Surveillance is thus viewed as a critical component of coercive control, used to hold power over targets with the threat of violence for noncompliance"*. The surveillance capabilities and opportunities for micro-regulation conferred by modern telecommunications applications, e.g. a notification on a joint banking app, tracking information on an internet connected car, a tracking device on a set of keys, a smart doorbell that alerts the attacker when the target is leaving the property, for example, enables an attacker to establish a sense of omnipotent omnipresence in the targets' life. Those attackers who seek to misuse telecommunications applications in this way can be considered dangerous to the psychological, emotional, financial and physical well-being of the targets.

By understanding how omnipresence is established and how it evolves, it may be possible to mitigate this troubling aspect of consumer IoT facilitated domestic abuse. Research into attacker omnipresence has found four characteristic phases of consumer IoT/technology facilitated domestic abuse. Attacker omnipresence tends to follow a typical temporal sequence that starts with "establishing omnipresence" through consolidation of control of the technology and user accounts. Once omnipresence is established, attackers engage in "covert omnipresence" involving surreptitious surveillance along with "overt omnipresence" characterized by unconcealed efforts to control, harass and intimidate using technology. When an individual attempts to end the relationship, attackers typically "change the project" from trying to keep the target engaged in the relationship to destroying them for leaving it. At this stage attackers switch to "retributive omnipresence" seeking revenge and humiliation by any available means now greatly facilitated by the plethora of available technologies that can be misused to survey and harass an individual through a multitude of channels long after physical separation is established.

Examples of omnipresent behaviour as identified in table 2.

Table 2: An Overview of Omnipresent Behviour [i.21]

Types of Omnipresent Behaviour	Examples of the Omnipresent Behaviour
Establishing omnipresence	Attackers openly seek information and access early in the relationship framed as care, concern, sharing and a sign of commitment. Attackers are account holders for family plans set passwords. Device mirrored to keep track of targets. Sets up an account for the target on attackers' own computer and watches the target enter the password. Joins target network on social media later used to harm personally and professionally. Installs CCTV cameras around the home. Turns on location tracker on targets phone to make sure they are OK getting the bus.
Overt omnipresence	Attacker checks target phone in front of them. Dozens or hundreds of calls and text messages. Installs CCTV cameras and then texts to ask, "What are you watching on TV?". Spoofs phone number to bypass blocking. Demands target answers immediately or else is punished.

Types of Omnipresent Behaviour	Examples of the Omnipresent Behaviour
Covert omnipresence	Happens in tandem with overt omnipresence, continuing and intensifying after separation. Checks text messages without permission. Installs spyware. Dual-use tracking capability misused. Draw upon intimate knowledge of partner to guess passwords to access account. Proxy stalking through friends and family even when blocked, e.g. looking for tagged photos. Creates fake profiles in target's name to gather information about them. Plants GPS on vehicle to keep track of target often after separation when they no longer have smartphone access. Emerging risks around consumer IoT used to spy on partner. Attackers with legal rights to see child after separation use children's phones, games consoles or other devices as a means to monitor the target post-separation.
Retributive omnipresence	Attackers "change the project" from attempting to keep their target in the relationship to destroying them for leaving it. Switches from in person one-to-on to public behaviours aimed at humiliation, reputational damage, and isolation from potential support. Calls and texts the target incessantly, but the volume increases, and content alternates between abuse and professions of love. Threats of suicide or self-harm. Commissions others to assist in the abuse including new partners, friends, or relatives. Attackers control the narrative around abuse. Steals targets phone and writes to all their Facebook friends to inform them that they had left them, adding 'I don't know what happened to them. They're not mentally okay'. Hijack targets' online accounts, deactivating and interfering with them, preventing targets' from using them. Delete important emails and important official documentation. Impersonation online. Distributed Denial-of-Service (DDoS) attacks on targets' network address. Fake profiles on dating sites encouraging humiliation of targets. Crowdsourcing to harass under guise of finding a relative. Revenge porn sites to upload images and survivor's contact details. Doxing.

6.3 Potential Strategies for Coercive Control Resistant Design to Prevent Harm

6.3.1 Visualization of the proliferation of personal data

The target typically has a digital footprint that comprises a complicated series of entanglements between the accounts and devices held by the target, the attackers, and the associates of the attacker including children and other family or friends, which can result in exposure to a complicated set of attack vectors for abuse that may be non-obvious. The proliferation of hidden connections and leakage of personal information between devices and accounts in a consumer IoT ecosystem is potentially extremely hazardous in a situation of domestic abuse. This is compounded by the complicated and hidden nature of the potential connections to the attacker that may be opaque to the target.

To address this issue, research into clinical computer security for targets of domestic abuse have identified the utility of producing a visualization of the digital footprint and digital entanglements of the users (targets) they refer to as a "technograph". The technograph is defined as: "A visual map loosely inspired by genograms, a technique used by clinicians in medicine and behavioural health to map family relationships and histories [i.16]. The technograph uses shapes and symbols to visually document relationships between (1) devices, (2) accounts, and (3) people (usually the client's family). Drawing connections between entities can give the designers a clearer picture of potential sources of risk from their consumer IoT devices [i.22].

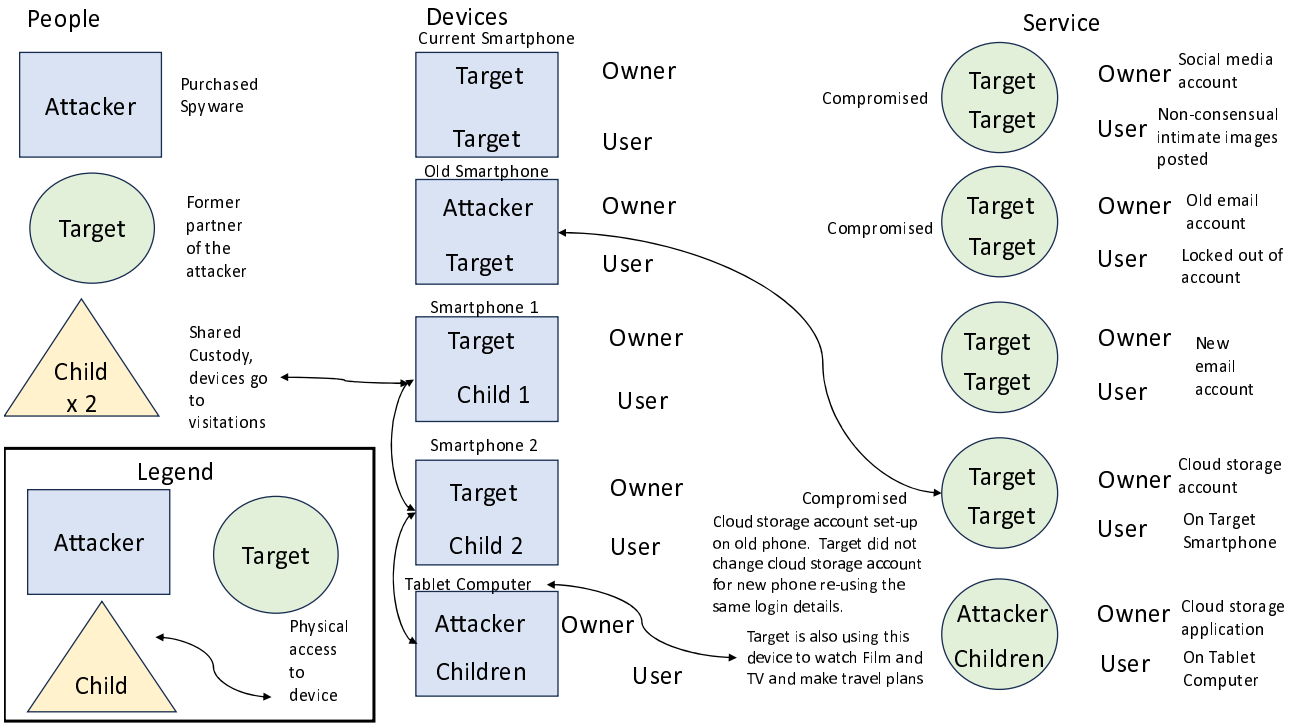

Figure 1: A hypothetical simplified example of a technogram illustrating the digital footprint and entanglements of the target and their children with an attacker

Figure 1 shows an example of a technograph. Currently such diagrams are produced in a non-automated fashion by support workers assisting a client experiencing technology facilitated domestic abuse in certain pioneering assistance programs. This approach can be particularly helpful to identify when an attacker may have indirect access to the target's digital assets, e.g. when family plans synchronize data across devices and accounts. Potential unintended exposure of private information to the attacker needs to be easily recognizable in a visual format that provides clues to potentially non-obvious vulnerabilities. With the advent of consumer IoT, the complexity of entanglements is likely to become intractably complex and obscure to manual investigation through recollection alone potentially placing targets at increased risk of abuse.

6.3.2 Example: of children & in coercive control

Children can be the targets of technology-enabled coercive control [i.23] and are harmed by the non-physical abusive behaviours inherent to coercive control-based domestic violence, including continual monitoring, isolation, and verbal/emotional/psychological and financial abuses [i.24]. It should be noted that this situation equally applies to cases where one person has control, guardianship, power-of-attorney, etc. over another person regardless of age or relationship (e.g. foster teens [i.55]).

Coercive control can affect children in similar ways as adults, leading children to feel confused and afraid, living constrained lives, and being entrapped and harmed by the attacker. This affects children and young people emotionally/psychologically, physically, socially, and educationally.

In abuse cases where an intimate partner physically escapes their attacker, attackers may continue coercive control against their children or by using their child in stepping stone attacks to get to the partner who escaped, including "violence, threats, intimidation, stalking, monitoring, emotional abuse, and manipulation, interwoven with periods of seemingly 'caring' and 'indulgent' behaviour as part of the overall abuse" [i.25]. In this case, that child has the "access to other at-risk users" risk factor from Warford et al.'s framework [i.53] (in this case, the child has access to the target who happens to be their parent). Children brought up in family systems affected by coercive control experience long term problems. Common tactics include monitoring and stalking; threats and intimidation and blocking communication. These harms have been perpetrated using mobile phones; texting; social media; GPS tracking-enabled devices and spyware [i.23]. It causes real harm, negatively impacting children's mental health (67 % of cases), their relationship with the non-abusive parent (59 %) and their everyday activities (59 %).

In cases of domestic abuse, co-involvement of children can become particularly intense and damaging post separation. When the target attempts to leave, the attacker often escalates abuse, harassment, and violence towards them and "changes the project" from attempting to keep them within the relationship to destroying them for leaving it [i.26]. At this time attackers engage in retributive omnipresence using technology [i.21]. Technology is now a key mechanism for attackers to extend control beyond the bounds of the relationship, and that may intensify targeting of children. Upon separation the attacker adopts an increased focus on the abuse, control, and harassment of the children as a means to continue to exert control over the mother, manipulating legal expectations for continued child contact using technology [i.27], [i.28]. Coercive control is deployed post-separation using commonplace technology, e.g. instant messaging, text messaging, phone calls, social media, as well as tracking devices, spyware, with emerging issues over ongoing access to home IoT systems, routers, and spying using internet connected toys or speakers, manipulating child contact to gain access to continue the abuse of the mother resulting in ongoing trauma and entrapment. Technology-facilitated abuse continues and escalates as couples separate given that avenues for control and physical violence change with technology seen as an alternative to in person contact. Post-separation co-parenting arrangements provide ample opportunities for technology-facilitated abuse. Attackers' contact with children via technology, whether mandated by court order or voluntarily enabled by adult targets, could expose children to abusive behaviour. Technology providers should be aware that novel technologies, such as IoT devices, could be misused by attackers in these situations, e.g. internet connected toys to spy on and track children and their mothers or be used in attempts to create false evidence of bad parenting. It is important that technology providers consider the landscape of risk both within the relationship and post separation and understand that technology is intimately implicated in intensified forms of abuse and control of both women and children post separation.

6.3.3 Implementing Coercive Control-Resistant Design

6.3.3.1 Introduction

There are certain steps consumer IoT designers can make which will enable them to implement coercive control resistant design into their products by raising their awareness of user safety concerns and needs and expanding threat modelling to account for interpersonal harms [i.36], [i.38], [i.39]. Designers and developers of consumer IoT products have a responsibility to fully understand how they impact the lived experiences of targets facing coercive control. Otherwise, they risk unwittingly assisting the attackerT.

6.3.3.2 Online Harms Policy

There is an expectation from user that companies will have measures in place to ensure duty of care to keep their users safe from harm:

1) Companies should take steps to ensure their services are safe, including outlining measures to ensure device and service platform for users have easy to use tools to control the privacy and visibility of their accounts and are able to control access to them.

2) Tools to help users experiencing harassment, such as the ability to report, block or stay hidden from other users.

3) Measures to prevent banned users creating new accounts to continue harassing their target.

4) Steps to ensure that users who have experienced harassment are directed to, and can access, adequate support.

6.3.3.3 Security and Safety of Consumer IoT design

There are broad overarching security requirements designer should implement:

1) No universal default passwords in consumer smart products.

2) Device producers should establish and maintain a vulnerability disclosure policy. This means there would be a clear route for users to report security vulnerabilities when they are discovered, and a process for remediation.

3) The device producers should explicitly state how long a product will receive software security updates for.

4) Threat modelling paired with usability analysis for the design and development of safer systems.

5) Incorporating privacy and security by default, during the design process.

6) Companies should get users' permission before collecting and sharing location data. So, this could mean disabled by default. Also, they should inform users how they can stop the collection of such information, and its deletion if requested which is under GDPR right to be forgotten.

6.3.3.4 Technology Design

There are key principles designers may incorporate:

1) Diversity. Ensuring a diverse design team to broaden the understanding of user habits.

2) Privacy and choice. Allowing users to make informed choices about their privacy settings.

3) User Awareness. Making it clear when settings have been changed and how this affects the functionality of the devices.

4) Security and data. Ensuring that products only collect and share necessary data, limiting the risk that data are used maliciously.

5) User Experience. Giving users greater confidence to use technology by making it simpler to understand, limiting the risk of attackers exploiting a target's lack of technical ability.

6.3.3.5 Education and Resources

A number of organizations have produced guidance on the safe use of technologies and how individuals can implement better privacy protections. Some organizations have also produced specific guidance on technology abuse for the targets (victims) and professionals working with targets (victims). These include guidance on how to document technology abuse, information about spyware and surveillance, and guidance on privacy and security features of social media platforms.

Examples of these resources can be found at these links:

- National Network to End Domestic Violence (NNEDV) Safety Net Resources
- Refuge
- UCL
- VAWnet
- SafeLives
- National Network to End Domestic Violence
- National Center for Victims of Crime.
- Get Safe Online
- GSMA (Children and Mobile Technology) (Safety, privacy and security across the mobile ecosystem)

NOTE: These are links to organizations and resources in the UK, USA and a broad global coverage respectively ideally provided resources should be country and/or region specific as to where a product/service is marketed and sold.

6.3.3.6 Role Technology can Play in Supporting Targets

Technology can offer a lifeline to targets, enabling them to access support services and information. It can also provide a way for them to record evidence of their abuse. There are different ways in which technology may help targets including:

1) Finding information. Targets may use internet searches to access information about domestic abuse, such as information and advice about abusive relationships, legal and financial information, and advice on safeguarding children and support services.

2) Accessing support services and networks. Targets may use the internet to connect with domestic abuse support services, including those offered by charities and local authorities. There are several charities offering an online live-chat service for accessing support. Technology can also enable targets to communicate with their own social network for help.

3) Connecting with other targets. Social media support groups and forums allow targets to connect with each other and find emotional support.

4) Gathering evidence. Technology may also help targets gather evidence of domestic abuse. For example, using a phone as a recording device or forwarding incriminating emails. Specific apps are available to help targets record evidence, which can include providing a secure diary function for targets to document their abuse. Additional information about using digital material in legal proceedings can be found in ETSI TS 103 643 [i.67].

5) Protecting and alerting targets. A range of technology solutions exist that aim to help protect targets, including specially designed devices and apps. Some private companies (mostly US-based) have developed 'wearable' panic alarms that are easy to hide or disguise. Apps and software also exist that can prevent a target being monitored with stalkerware by detecting and removing stalkerware from a person's device.

The way technology can support targets varies depending on what stage of an abusive relationship they are in. For example, if a target is in the early stages of an abusive relationship, they may use online information to help them determine whether their relationship is abusive, while a target in the process of leaving such a relationship may use technology to gather evidence about their abuse.

While technology offers access to information and support, a target's circumstances and the complex dynamics of their abuse may limit how easily they can use it. For example, it has been highlighted that often targets only have a short time window to access information or contact support services, but there is a risk of online information being difficult to find, duplicated or does not answer their key questions. Also, information can be lacking such as financial and legal information. While technology can play an important role in helping targets to find information and support, it does not replace face-to-face interactions with services or other targeted survivors.

7 Trauma Informed Design

7.1 Introduction

Trauma Informed Design can be defined as recognizing understanding how people's trauma affects their experiences. It is important to recognize and understand that trauma is the physical, emotional, or psychological harm caused by deeply distressing experiences [i.13]. The informed design is seeking to avoid exacerbating this trauma in the process of discovery and design and creating solutions which could make a positive impact to their recovery [i.11]. There are different factors that can inform trauma informed design. These are:

1) Enable users to secure privacy from an intimate attacker in threatening situations.

2) Ease of use of personal security functions.

3) Common design of personal security functions across devices and applications.

4) Information transparency, including who can see what information exists of the user, when and where easily accessible and standardized.

5) Consideration of degree of danger, likelihood of escalation of abuse, impact of target blaming, deleterious impacts on ability to self-advocate, emotions, cognition, and execution of complex tasks due to abuse.

6) Useful onward help signposted appropriately.

The impact of trauma should be considered in the design of user interfaces and functionality for those experiencing coercive control. Those subject to Consumer IoT-enabled stalking, harassment or coercive control need to understand and have control over user interfaces to secure their personal safety in a high threat situation. Sudden drastic changes to the user interface mean that target will not be able to find essential functionality or to secure their personal data from the attacker. An example of unintended harm considers sudden, drastic changes to the user interface of a co-parenting application that gives the impression that written entries about the abuse may now be visible to everyone including the abusive ex-partner. Even if this is not the case, sudden, confusing changes in the user interface could lead a target to delete their written entries fearing they are now visible to an abusive partner thereby harming their case to prove coercive control because the evidence no longer exists. In general, security features that allow someone to secure or hide their personal data need to be prominent, easy to use, ideally standardized across applications and not subject to change, i.e. with static functionality and layout.

7.2 Design Principles

Trauma-informed design includes the personal interaction between the abused person and the company contacts responsible for customer service with the target, and any helping interventions such as a chat bot trained to deal with an abusive situation to provide information to a person.

Some trauma-informed principles are relatively simple to create a simple, visually appealing welcoming atmosphere with straightforward language for the user interface. The most difficult area to grasp, which requires specialized knowledge, is the area of interpersonal interaction with the target. Without trauma-informed expertise, there is a high risk of re-traumatization of the individual when they seek help. As researchers note that *"Too often, well-meaning individuals participate in a system that retraumatizes targets of childhood abuse and interpersonal violence"* [i.19].

7.3 Relational Safety Principles

Relational safety needs to be established with the target that are mindful of the complex deleterious effects of abuse. In general, relational safety involves establishing trust, transparency, safety, and predictability and could look like:

- Non-judgmental validation of a person's experience of abuse.
- Non-judgemental validation of the target's choices in how to deal with the abuse.
- Reinforcing the idea that they are the person best placed to know what is best for them.
    - In this regard, be aware that due to the destruction of the internal listening boundary in emotional abuse and the inherent power imbalance in the helper-helped relationship, the target may experience advice as a demand, rather than seeing it only as a proposed suggestion as an option. Communications needs to be delivered in such a way as to minimize the risk that the target feels compelled to follow advice, and to empower the person involved to understand that they are best placed to decide what is best for them and make their own independent choice as to what is right for them. Companies need to be extremely careful about what advice they give as a target may put more weight on suggestions provided by the helper than on their own best judgement.
- Clear boundaries with clearly defined roles for the helper. This includes communicating to the person experiencing coercive control that they have the right to set limits or end the interaction.
- To provide this level of care, those directly involved with targets of abuse at a minimum need to be emotionally mature and able to contain the potentially strong emotional affective states of the abused person without emotional reactivity, criticism, giving advice or becoming defensive to avoid re-traumatization. Training in the effects of trauma or bringing in trauma-informed professionals is needed.

7.4 Policy Guidance

In relating to targets, the companies need to avoid:

- Taking the power-over stance in the helper-helped relationship.
- Implying that the person does not know what is best for them.

- Shaming.
- Victim blaming.
- Denial and minimization of the abuse.
- Implying that the abuse is understandable.
- Implying that trauma symptoms mean there is something wrong with the person.
- Emotional reactivity and any interpersonally abusive behaviours which are even more damaging for someone who has experienced relational trauma.

Overall, companies should seek to support the target in reaching an independent decision in their own best interests rather than being told what to do and do their best to avoid re-traumatization by seeking expert input on how best to provide this support.

7.5 Customer Support Guidance

The training of frontline agents/customer support staff to be better prepared for tech enabled attack cases is critical for supporting the targeted users. Equipping customer support agents with a basic understanding of Consumer IoT/Technology enabled abuse and the caution needed for a proper response is also vital to prevent inadvertent harm, such as escalating abuse by removing spyware without further precautions or making misleading promises.

NOTE: Further guidance on Customer Support can be found in ETSI TR 102 202 [i.30]. It reviews problems associated with call centre work are highlighted, and where appropriate, examples of best practice are given to illustrate how they may be avoided.

- Introduce Consumer IoT-Enabled Coercive Control to customer support agents. Discuss the prevalence of it, including how the technology is misused to facilitate abuse and non-technical aspects (e.g. the targets and attacker's social entanglements and the need for holistic safety planning). Explain why agents should be committed to learning how to support the targets.
- Describe common consumer IoT abuse and desired responses. Present scenarios of how attacker exploit technologies in coercive control and model how agents should respond. Define and give examples of trauma-informed language and explain its importance. Frame the problem as an opportunity to offer help rather than a situation that requires careful vetting or evaluation of the customer's victimhood.
- Explain how agents could provide support. Present methods for assisting targets, such as asking questions that consider broader risks beyond the immediate tech issue, sharing tech safety resources, and making referrals.
- Identify mental health resources for customer support agents. Provide resources (e.g. therapeutic sessions and peer support groups) for agents who might be experiencing coercive control or suffering secondary trauma from handling such cases.

The training should make customer support agents aware of unique risks and nuances in consumer IoT enabled coercive control, help them pick up cues that indicate customers experiencing coercive control, and teach them how to share resources safely and respectfully.

Annex A:
Defining the difference between Safety and Security

Although there may be little difference between feeling secure and feeling safe on a daily personal basis, the concepts of safety and security are not fully analogous, though providing clear definitions of the concepts remains a challenge. Not only is there a single word for safety and security in many languages (unlike in English), but also the many definitions from academics on the one hand and the colloquial use of the terms on the other hand convey ambiguities.

EXAMPLE: English: Safety/Security; French: sécurité/sécurité; German: Sicherheit/Sicherheit. If context specific in German: Funktionale Sicherheit = safety (functional safety).

The definitions provided by academics mainly refer to two types of distinctions between safety and security: one related to the intentionality, safety focusing on hazards and non-intentional or accidental risks as opposed to security that focuses on malicious threats and intentional risks. The other one builds on the differences of origins - consequences, safety being the ability of the system not to harm the environment whereas security is the ability of the environment not to harm the system.

Despite efforts at refining the distinction between safety and security, a returning question is whether to distinguish the two or to best manage dangers overall whether they make people feel unsafe or insecure. A central concept for how to achieve both safety and security is risk management. However, there is much confusion as to what to expect of risk analysis, i.e. what are they identifying, how it can be carried out, i.e. conduct one risk analysis for the security risks and one for the safety risks or both together as they may impact each other, and if it is the same for safety and security [i.8].

Annex B:
What is abuse?

The World Health Organisation (WHO) defines domestic abuse as: *"a pattern of behaviour in any relationship that is used to gain or maintain power and control over an intimate partner. Abuse is physical, sexual, emotional, economic, or psychological actions or threats of actions that influence another person. This includes any behaviours that frighten, intimidate, terrorize, manipulate, hurt, humiliate, blame, injure, or wound someone".*

The WHO, like many other organizations understand domestic abuse within a feminist framework. Historically known as the power and control wheel [i.48] and increasingly called the coercive control wheel, it helps explain the power dynamics in intimate and familial relationships. In this model, the wheel is similar to that of a bicycle; it consists of a hub at its centre and spokes reaching to the outer tyre. In this analogy the hub of the wheel represents the attackers' desire to maintain power and control in their relationships (see figure B.1).

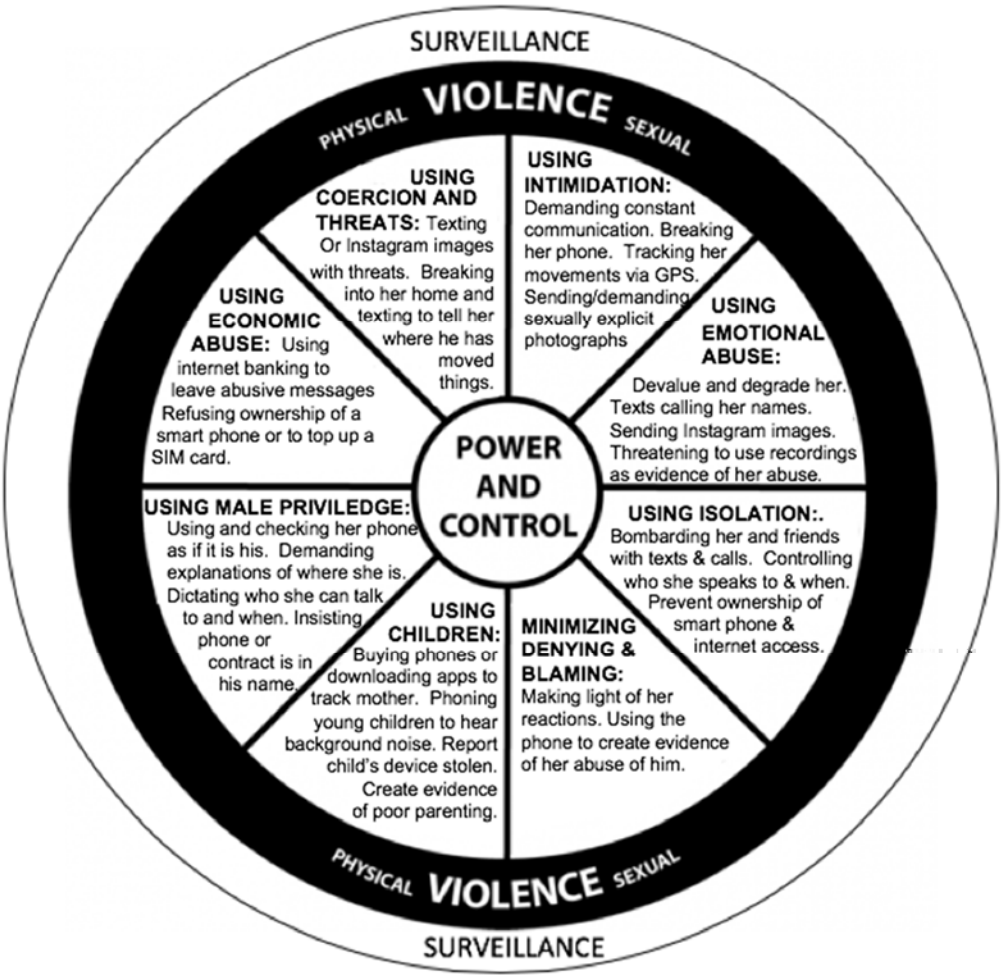

Figure B.1: Coercive Control Wheel

The spokes of the wheel represent behaviour exerted by the attacker, to compel someone to do something they do not want to do and/or prevent them from doing something they do want to do [i.49]. These attacker behaviours are deliberate, pose a credible threat and cause fear in the target. This fear is based on what could happen [i.50]. Tactics include emotional violence (including humiliation), denying, minimizing, excusing, and blaming, intimidation, isolation (including monitoring and controlling), coercion and threats [i.51]. They are not isolated incidents but cumulate over time. Several behaviours can also be performed in only one incident [i.52], [i.48].

The black tyre represents either the physical /sexual violence that will occur or the threat of such violence if the target fails to comply. It is the fear of what might happen that maintains the power and control represented by the hub of the wheel.

The wheel provided in figure B.1, relates to the role of technology in the coercive control of heterosexual women who had fled their abusers. The examples provided in the spokes of the wheel are how attackers use mobile 'smart' phones, the gateway to IoTs, to extend the reach and impact of the abuse.

Annex C: Bibliography

- Afrouz, Rojan. "The Nature, Patterns and Consequences of Technology-Facilitated Domestic Abuse: A Scoping Review", Trauma, Violence, & Abuse, Sept. 2021.
- Bailey, Jane, et al. "Technology-Facilitated Violence and Abuse: International Perspectives and Experiences", The Emerald International Handbook of Technology-Facilitated Violence and Abuse, edited by Jane Bailey et al., Emerald Publishing Limited, 2021, pp. 1-17.
- Barter, Christine, and Koulu, Sanna. "Digital Technologies and Gender-Based Violence - Mechanisms for Oppression, Activism and Recovery", Journal of Gender-Based Violence, vol. 5, no. 3, Oct. 2021, pp. 367-75.
- Coombs, Elizabeth. "Human Rights, Privacy Rights, and Technology-Facilitated Violence", The Emerald International Handbook of Technology-Facilitated Violence and Abuse, edited by Jane Bailey et al., Emerald Publishing Limited, 2021, pp. 475-91.
- Dragiewicz, Molly, et al. "Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms", Feminist Media Studies, vol. 18, no. 4, July 2018, pp. 609-25.
- Dragiewicz M., Harris B., Woodlock D., Salter M., Easton H., Lynch A., Campbell H., Leach J., Milne L. "Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime", The Australian Communications Consumer Action Network (ACCAN), 2019.
- Hand T., Chung D., Peters M. (2009). "The use of information and communication technologies to coerce and control in domestic violence and following separation", Australian Domestic and Family Violence Clearinghouse, UNSW SydneyAU.
- Brown C., Hegarty K. "Development and validation of the TAR Scale: A measure of technology-facilitated abuse in relationships". Computers in Human Behavior Reports,3, 100059, 2021.
- Drouin M., Ross J., Tobin E. "Sexting: A new, digital vehicle for intimate partner aggression?", Computers in Human Behavior,50, 197-204, 2015.
- Henry N., Flynn A., Powell A. "Responding to 'revenge pornography': Prevalence, nature and impacts", Criminology Research Grants Program, Australian Institute of Criminology, 2019.
- Woodlock D., McKenzie M., Western D., Harris B. (2019). "Technology as a weapon in domestic violence: Responding to digital coercive control", Australian Social Work, 1-13.
- Brown C., Hegarty K. "Digital dating abuse measures: A critical review", Aggression and Violent Behavior, 40, 44-59, 2018.
- Cuomo, Dana, and Natalie Dolci. "New Tools, Old Abuse: Technology-Enabled Coercive Control (TECC)" Geoforum, vol. 126, Nov. 2021, pp. 224-32.
- Baldwin, Susie B., et al. "Psychological Coercion in Human Trafficking: An Application of Biderman's Framework", Qualitative Health Research, vol. 25, no. 9, 2015, pp. 1171-81.
- Douglas, H., Dragiewicz, M., & Harris, B. "Technology facilitated domestic and family violence: Women's experiences", British Journal of Criminology, 59(3) 551-570, 2019.
- Evan Stark. "The dangers of Dangerousness Assessment", Fam. Intim. Partn. Viol. Q.2013; 6(2): 13-22.
- Nellie Bowles: "Thermostats, Locks and Lights: Digital Tools of Domestic Abusehttps://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html", The New York Times, June 23, 2018.
- Anna Moore. "'I didn't want it anywhere near me': how the Apple AirTag became a gift to stalkers", The Guardian Monday, 5th September 2022.

- Australian Government eSafety Research: "Children and technology facilitated abuse in domestic violence situations", December. 2020.
- "Safety Net Project - Exploring technology safety in the context of intimate partner violence, sexual assault, and violence against women", Evidence Collection Series: Internet of Things (IoT).
- Aaron James Webb. "Cyber Security of Smart Watches : A Review of the Vulnerabilities with Recommendations Presented to Protect the Wearables", International Journal of Network Security & Its Applications (IJNSA) Vol.14, No.3, May 2022.
- Lihi Dery, Artyom Jelnov and Antonio Fernández-Caballero. "Privacy-Accuracy Consideration in Devices That Collect Sensor-Based Information", Sensors (Basel). 2021 Jul; 21(14): 4684.
- Organisation for Economic Co-operation and Development: "Bridging The Digital Gender Divide Include, Upskill, Innovate", 2018.
- Albert, Leslie, Simon Rordan, Nitin, Aggarwal, Timothy Hill, 2019. "Gender and Generational Differences in Consumers' Perceptions of Internet of Things (IoT) Devices", e-Journal of Social & Behavioural Research in Business, Vol.10, Iss. 3, December 2019, pp: 41-53.
- Spluska, J; Tanczer, L. "Threat Modeling Intimate Partner Violence: Tech Abuse as a Cybersecurity Challenge in the Internet of Things". In: Bailey, J and Flynn, A and Henry, N, (eds.) The Emerald International Handbook of Technology Facilitated Violence and Abuse. (pp. 663-688). Emerald Publishing Limited, 2021.
- Foucault, M.: "Crime and punishment: the birth of the prison", Penguin, London, 1991.

Annex D:
Change history

Date	Version	Information about changes
December 2023	V0.0.1	Final Draft

History

Document history		
V1.1.1	January 2024	Publication