Technology facilitated abuse and the security paradox

Alice Hutchings
Department of Computer Science & Technology
University of Cambridge
Cambridge, UK
alice.hutchings@cl.cam.ac.uk

***Abstract*—Computer security is built around protecting systems from unauthorised users. But in intimate partner violence, it is often the admin who is the threat. By failing to differentiate between 'care' and 'control', the tech industry has effectively built an infrastructure of coercion. This creates a security paradox: the very features designed to provide security (for the home, device, or user) are weaponised as vectors for insecurity for the survivors of intimate partner violence. Mainstream technologies enable abusers, while survivors are expected to manage their own safety with limited tools. To resolve this, we must move beyond performative safety features that place the onus on survivors to manage their own protection. I call for a paradigm shift, towards safety by design, whereby developers anticipate abusive users and integrate privacy protections by default.**

***Index Terms*—Technology facilitated abuse, intimate partner violence, infrastructure of coercion, safety by design**

The computer security industry can be thought of as guardians who battle against external adversaries trying to misuse or gain access to technical systems. The assumption is that the 'enemy' is distinct from the 'user'. Firewalls, encryption and access control keep out the baddies and protect the authorised users. What then happens when the 'baddie' is the account holder, the bill payer, and the device administrator?

When we adopt the assumption that 'users are good', we fail to account for abuse that is not directed towards the technology, but uses that technology to cause harm to other people. Rather than abusing the technology, they are using it *as intended* in ways that abuse others. By failing to recognise that abusers regularly use standard admin and user features to control, harass, and surveil others, the tech industry has inadvertently built an infrastructure of coercion.

Abusers are increasingly weaponising technology in intimate partner violence. In the digital home, security is often controlled by the abuser (the admin). Tools designed to provide security, peace of mind, or ensure the safety of minors are frequently misused by abusers to torment and control their victims. The market facilitates this, with stalkerware (mobile applications that enable covert surveillance) marketed for parental control, employee monitoring, or anti-theft purposes [1]. Disguising stalkerware as 'parental control' applications (often while still clearly advertising it to abusers) takes advantage of how we define legitimate oversight of minors.

We have normalised the infrastructure of coercion. Tracking and surveillance are viewed as legitimate features for finding lost keys (personal item tracking devices) or catching burglars (smart doorbells). Abusers use the technology features as intended, to track and to control [2]. Because the technology cannot infer intent, the admin is permitted to do as they wish. The abuse cannot be easily patched, leaving the technologies fundamentally flawed. Traditional defences fail when the abuser knows the password and is inside the firewall.

Security is designed to protect the user from the attacker. In domestic contexts, the abuser is often not only the user, but also the admin [3]. Admins are assumed to be benevolent and granted absolute power. User-centred design also fails survivors when the user is the abuser. Features such as being able to 'drop in' to a microphone-enabled device/smart speaker, or access a doorbell's live feed, directly facilitate abuse. Abusers do not need technically sophisticated attacks to enable their abuse [4]. Modern tools and devices make abuse straightforward. Abusers use features like *Find My*, activity logs, and alerts exactly how they were designed [2].

Often in computer security the aim is to identify 'signatures' that indicate malicious behaviour. But we cannot detect this type of abuse simply by scanning for malware, as the tools of abuse are indistinguishable from the tools of care. Technically, parental care (tracking a child to ensure that they reach school safely) and intimate partner abuse (tracking a partner to spy on their activities) are indistinguishable. Because these behaviours are indistinguishable, we cannot patch the vulnerability without breaking the feature.

While Terms of Service may specify that the technology cannot be used to track people without consent, at the end of the day, it is the credit card of the purchaser that is being verified, not the consent of the person unknowingly being tracked. Furthermore, these terms contain legalese that is more about absolving liability than preventing misuse. And when abusers have control of the devices, privacy notifications and permission requests essentially become meaningless.

The onus is often placed on the victim to manage their own digital safety. This fails because the security protocols favour the (ab)user. Attempts to provide protection to users are often little more than safety theatre, with poor implementations. For example, before improvements were made to anti-stalking features associated with personal item tracking devices, to detect if you were being tracked, you would need to know what type of device might be tracking you, so that you could

download the corresponding app. Many of these also required manual scanning, so you would have to constantly scan in multiple locations to identify if unknown Bluetooth devices remained in your vicinity [2]. Likewise, our prior evaluations found many 'quick exit' buttons, often available on websites providing services for domestic abuse survivors, are poorly designed. In many implementations, it would be trivial for an abuser to discover the website the survivor was attempting to hide [5]. We give survivors a button and say 'here, save yourself'. But this is often little more than a placebo, as they lack the same technical power as the admin/abuser.

One of the fundamental assumptions of modern crime control is that *anyone* can be an offender. Rather than offending behaviour arising from some pathological state of the offender, it is assumed that offending behaviour can commence, and cease, depending on the particular circumstances surrounding an individual [6]. In relation to tech abuse, these circumstances may include what access they have to technology, the types of influence they experience, and their opportunities for abuse. Although this may make some people uncomfortable, as it might be preferable to demonise abusers as fearsome strangers, it has direct implications for how we design against abuse. If we view crime and abuse as predictable behaviour, we place it back under our control.

The tech industry should not be able to wash its hands of the problem by giving survivors a tool that is technically insufficient for the high-risk environments they are navigating. In some cases, even well-intentioned interventions can backfire, as the designers do not understand the abusive context. If an abuser discovers that a survivor is seeking help or attempting to conceal their digital tracks, it signals a challenge to their control and can be a catalyst for violence.

Often the most dangerous time for a survivor of intimate partner abuse is when the relationship ends. Relationship breakdown can also act as a catalyst for abuse [7]. The technology that entangles our day-to-day lives is making escape even more difficult. New 'safe' addresses can be inadvertently disclosed by mobile phones, vehicles, personal item tracking devices, earbuds, 'Find My' features, or online accounts. The admin retains permission by default, even when they do not have physical access to devices. The ways in which the survivor's safety is compromised may not be immediately apparent to them. Even if it is, the survivor either has to fight multiple opaque systems to revoke access or jettison the compromising technology, creating further burden.

The tech industry is enabling technology-facilitated domestic abuse, with features designed for users adopted by abusers. We need to move the responsibility for safety away from the survivor and towards the developers of the technologies that enable abuse. In some cases, the tech industry should reconsider their aversion to user friction. It should be hard for users to secretly monitor others, not seamless.

But we cannot rely on 'technosolutionism' to fix what are complex social problems. Technical fixes alone are like installing smoke detectors in a building without fire exits. As our technologies become increasingly automated and 'smart', avenues for misuse are likely to increase. As technology becomes enmeshed within our houses and workplaces, the user-centred model needs to shift accordingly. Rather than 'the user', technology needs to be built for 'the household' and 'the workplace', alongside the messy nuances of coercion and control that this entails. We need technologies that are built with the assumption that the admin may be hostile to prevent them becoming the tool of abuse. The deliniation between user and abuser should be removed, and instead recognise that abuse is the potential behaviour of *any* user.

Existing threat modelling frameworks such as STRIDE test how technical systems may be vulnerable to technical attacks. Industry also needs to consider how new technologies and features can be used for controlling, harassing, or surveilling others. The HARMS model (Harassment, Access and infiltration, Restrictions, Manipulation and Tampering, and Surveillance) is a new threat modelling framework [8]. It is designed to identify non-technical and human factors harms that are often missed by threat models that only focus on technical vulnerabilities. We focused on how everyday technology, such as IoT devices, can be exploited to distress, control or intimidate.

I conclude by calling for the tech industry to adopt safety by design principles. These should anticipate abuse, assuming that some users may be abusers and some might be under duress or monitored by the account administrator turned abuser. We need to move away from performative approaches and towards designing out abuse opportunities and providing actual privacy protections enabled by default.

Biography

I am Professor of Emergent Harms in the Security Group at the Department of Computer Science and Technology, University of Cambridge, and a Fellow of King's College. I am the Director of the Cambridge Cybercrime Centre, an interdisciplinary initiative uniting computer science, criminology, and policy to understand and disrupt cybercrime. My research focuses on online harms, abuse at scale, and the misuse of platforms and infrastructure. By analysing large-scale, real-world data, my work addresses urgent societal challenges, informs public policy, and supports law enforcement and industry partners. I am particularly interested in how digital systems shape risk, trust, and accountability in increasingly interconnected environments. My goal is to bridge disciplinary divides and drive evidence-based solutions to emergent harms.

Acknowledgment

This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) grant EP/T517847/1 and the European Research Council (ERC) under the European Union's Horizon 2020 research and innovation programme (grant agreement No 949127). I thank my colleagues at the Cambridge Cybercrime Centre, in particular Dr Kieron Ivy Turk, Professor Janet Davis, Hannah Pankow, and Professor Alastair Beresford for their thoughtful insights and detailed comments.

References

[1] A. Vijay, L. A. Saavedra, and A. Hutchings, "Catch me if you scan: A longitudinal analysis of stalkerware evasion tactics," in *Proceedings of the IEEE APWG Symposium on Electronic Crime Research (eCrime)*, 2025, pp. 1–16.

[2] K. I. Turk and A. Hutchings, "Spy-oT: Understanding how users learn to use internet of things devices for abusive purposes," in *Proceedings of the Twenty-First Symposium on Usable Privacy and Security (SOUPS)*, 2025, pp. 185–203.

[3] J. Slupska and L. M. Tanczer, "Threat modeling intimate partner violence: Tech abuse as a cybersecurity challenge in the internet of things," in *The Emerald International Handbook of Technology-Facilitated Violence and Abuse*. Emerald Publishing Limited, 2021, pp. 663–688.

[4] D. Freed, J. Palmer, D. Minchala, K. Levy, T. Ristenpart, and N. Dell, "A stalker's paradise: How intimate partner abusers exploit technology," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–13.

[5] K. I. Turk and A. Hutchings, "Click here to exit: An evaluation of quick exit buttons," in *Proceedings of the CHI Conference on Human Factors in Computing Systems*, 2023, pp. 1–15.

[6] D. Garland, *The culture of control: Crime and social order in contemporary society*. Oxford University Press, 2001.

[7] Q. Taylor, A. Talas, and A. Hutchings, "Love bytes back: Cybercrime following relationship breakdown," in *Proceedings of the IEEE APWG Symposium on Electronic Crime Research (eCrime)*, 2024, pp. 123–135.

[8] K. I. Turk, A. Talas, and A. Hutchings, "Threat me right: A human HARMS threat model for technical systems," in *Proceedings of the Security Protocols Workshop (SPW)*, 2025.