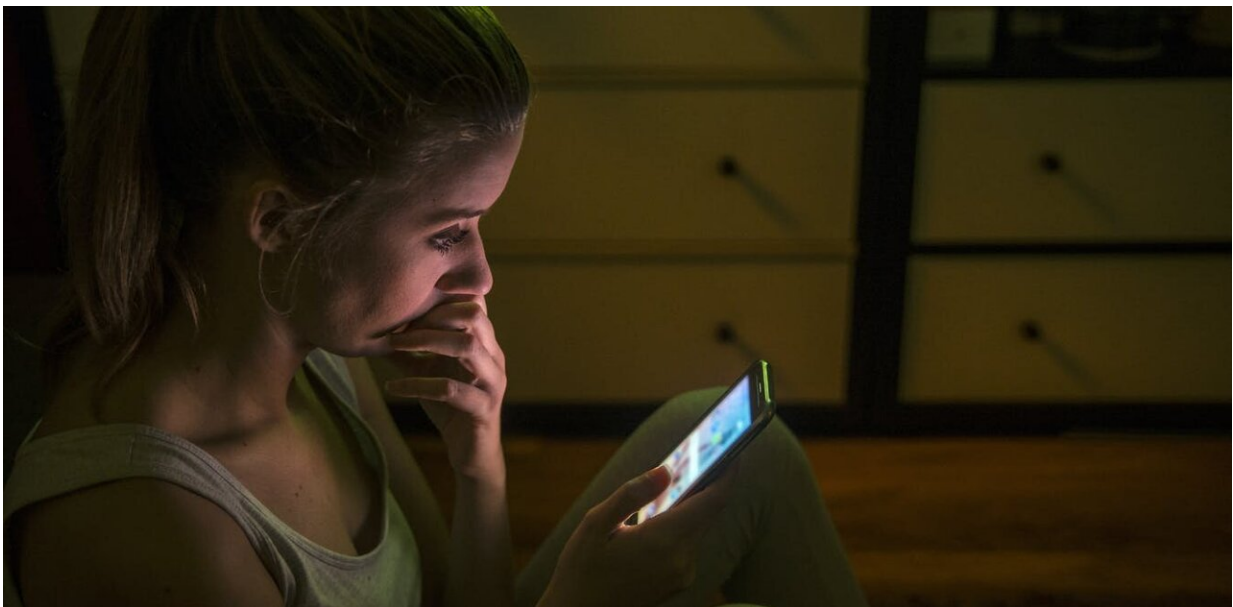


Technology-enabled abuse: How 'safety by design' can reduce stalking and domestic violence

November 11 2021, by Bridget Harris



Credit: Dragana Gordic / Shutterstock

Mobile phones and online technologies are frequently used by [perpetrators of domestic and family violence](#) to coerce, control and restrict the freedoms of victims and survivors.

Recent death reviews have found that [stalking by technology](#) and the use of fake social media identities are becoming more common elements in

cases of [domestic and family violence homicide](#).

In Australia, there are two leading agencies working to reduce this kind of technology-enabled abuse: [WESNET](#) and the [eSafety Commissioner](#). Both provide training for advocates and practitioners, as well as resources for victims and survivors. WESNET also provides [replacement phones](#).

Their work—and the "safety work" of people experiencing violence—is made more difficult by tech products and services that treat user safety as an afterthought. Platforms and the [tech industry](#) can do a lot to reduce harm by building in user safety from the earliest stages of product design.

Creating risk

At present, major tech companies often design and manage devices and digital media without considering user vulnerabilities.

[Until 2020](#), Google allowed [spyware and stalkerware](#)—software designed to be covertly installed on a phone to monitor and record photos, videos, texts, calls and other information—to be freely advertised on its platform. It banned the ads amidst mounting evidence that this kind of software is used to [enact intimate partner violence](#).

In April 2021 Apple released coin-sized tiles called AirTags intended to help people keep track of belongings via Bluetooth signals. After they were criticized as presenting a serious security risk by enabling [stalking of intimate partners](#), Apple [updated the devices](#) to make them beep at random intervals if they were away from the owner's phone.

Facebook's new smart glasses have also sparked [privacy concerns](#), like [Snapchat's Spectacles](#) and [Google Glass](#) before them. The glasses contain

cameras and microphones that enable (potentially covert) recording.

[Facebook did consult groups](#) such as the US National Network to End Domestic Violence in an effort to "innovate responsibly," though there are still concerns about how the glasses might be used.



Apple's AirTags had safety features added after release following criticism.
Credit: Jack Skeens / Shutterstock

Recognizing user realities and threat

Traditional ideas of cybersecurity are focused on "stranger threats."
However, to reduce and combat digital domestic and family violence we need an "intimate threat" model.

Partners and family can compel others to provide access to devices. They may be linked to online accounts or able to guess passwords, based on their intimate knowledge of the owner.

In this context, technologies that enable surveillance and recording can be used to constrain and threaten victims and survivors in alarming ways, in everyday life.

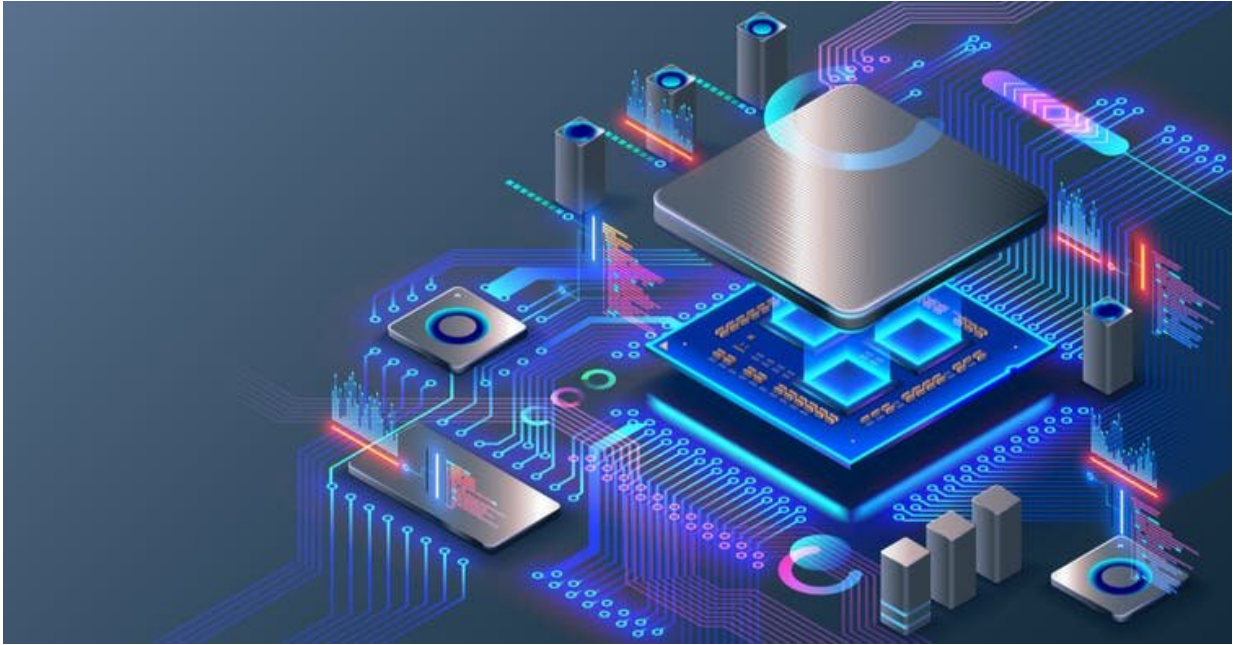
Understanding and seeking to alleviate risk posed by abusers requires platforms and industry to think proactively about how technologies may be co-opted or weaponised.

Safety by Design

The eSafety Commissioner's [Safety by Design](#) initiative aims to make user safety a priority in the design, development and deployment of online products and services. The initiative revolves around three basic principles.

The first is that service providers are responsible for making user safety the number one priority. This means platforms and other companies work to anticipate how their products may facilitate, increase or encourage harm. In this way the burden of safety will not fall solely on the user.

The second is that users should have power and autonomy to make decisions in their own best interest. Platforms and services should engage in meaningful consultation with users, including diverse and at-risk groups, to ensure their features and functions are accessible and helpful to all.



‘Safety by design’ makes user safety the top priority in the design of new products and services. Credit: Shutterstock

The third principle is transparency and accountability about operations and published safety objectives is essential. This also helps users to address safety concerns.

There is growing support for these principles among tech companies. Last year IBM published its own guide to "[coercive control resistant design](#)".

Effective approaches must also acknowledge how intersecting or overlapping forms of structural or systemic oppression shape an individual's experience of technology and can deepen social inequalities.

To realize the goals of [safety](#) by design or coercive control resistant

design, we will need to review not only the policies but also the actual practices of platforms and industry, as they emerge.

How tech can improve

eSafety has produced [Safety by Design assessment tools](#) to improve and innovate based on good practice and evidence-informed resources and templates.

Platforms and industry have a key role to play in addressing the impacts of domestic and [family violence](#) through [design](#). They can and should do more in this space.

This article is republished from [The Conversation](#) under a Creative Commons license. Read the [original article](#).

Provided by The Conversation

Citation: Technology-enabled abuse: How 'safety by design' can reduce stalking and domestic violence (2021, November 11) retrieved 21 March 2023 from <https://phys.org/news/2021-11-technology-enabled-abuse-safety-stalking-domestic.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--