Five Technology Design Principles to Combat Domestic Abuse

By Lesley Nuttall, IBM UK, Academy of Technology

In response to a global surge in domestic violence, leading to a UN call for measures, IBM proposes five design principles aimed at combating a new breed of domestic abuse—technology-facilitated coercive control.

Our tech ecosystem is teeming with innovators who constantly bring us products and devices that improve lives. In a COVID-19 world where self-isolation has become the norm, we have gained a new appreciation for technology's ability to bring us together and enhance our wellbeing. While there is no doubt that technology has tremendous potential for good, providing a mechanism for increased connection and protection, the sad reality is that bad actors can exploit it to cause real-world harm. The same technologies that safeguard us, ease our routines, and enrich our experiences are being manipulated by abusers to exert control over their victims. This weaponization of technology is particularly prevalent in domestic abuse, especially coercive control—a relentless pattern of controlling behaviour aimed at instilling fear and compliance in a victim.

Domestic abuse is a pervasive problem in society that affects both developed and poorer economies. In the United States, 1 in 3 women have experienced physical violence from an intimate partner,[1] and in parts of sub-Saharan Africa, partner violence is thought to be a reality for 65 percent of women.[2] An EU-wide survey indicated that 22 percent of women have experienced violence by a partner.[3] What is deeply worrying is that a recent UN report exploring the impact of COVID-19 on women highlighted a trend of increased abuse as homes are placed under strain from self-isolation and lockdown.[4] This has become so widespread that UN chief António Guterres is calling for measures to address this "horrifying global surge in domestic violence."[5]

1 in 3

women worldwide have experienced intimate partner violence.

(SOURCE: WHO)

Abusers are adept at leveraging anything at their disposal to further their own ends, and this includes technology. While the methods of technology-facilitated abuse are wide-ranging, what is particularly insidious is that applications designed with the best of intentions are being leveraged for malevolent purposes.

Experts estimate a **20 percent increase** in domestic violence cases during COVID-19.

(SOURCE: UN REPORT)

A couple of examples:

- **The connected doorbell app that allows you to remotely see who is at the door was built with safety in mind. However, the motion capture functionality can be used to monitor and entrap victims, with instant notifications being sent when an attempt is made to leave the home.**

- **The credit card app that provides purchase notifications was built to help combat fraud. However, its use can give enhanced control over victims with details of their spending being constantly monitored.**

With cases of technology-facilitated domestic abuse on the rise, this is not a niche issue. There have been numerous articles and reports of survivors' experiences. A recent UK news investigation found an 1,800 percent increase in alleged cyber stalking offences between 2014 and 2018. An Australian survey of domestic abuse support workers found an almost complete overlap between technology abuse and domestic abuse with 98 percent saying they had clients who had experienced technology-facilitated abuse. In addition, Refuge, which runs the UK's domestic abuse helpline, reported that nearly three-quarters of the people seeking their help last year had faced abuse via technology.

Technology-facilitated abuse is a challenging issue, and there is no simple solution to eliminate it. However, by making subtle decisions—balancing intended with unintended consequences—it is possible to design technology to be resistant to it. To aid technologists in making these decisions, IBM is proposing **five key design principles** to make products resistant to coercive control.[6]

Creating products that do not contribute to, or enable, society's problems is an ethical responsibility of all companies—not only because it is the right thing to do but also because it is the best business approach. A recent study found that 80% of global respondents agreed with the statement that corporations have a responsibility to prioritize their employees, the environment, and their community as much as they prioritize delivering profits to their shareholders. Focusing on values and purpose has been IBM's approach for more than a century, with these design principles being the latest example of IBM's desire for technology to shape lives and society for the better.

By sharing this set of design principles, IBM aims to improve the usability, security, and privacy of new technologies to make them inherently safer. We recommend that these become an integral part of any product design review. While these principles may be familiar to technologists, they take on additional meaning when looked at through the lens of coercive control.

Five Key Design Principles

1

Promoting Diversity

Having a diverse design team broadens the understanding of user habits, enabling greater exploration of use cases, both the positive and the negative. Often when developing a new technology, designers have target users in mind. However, they might not be the only type of users that end up using the technology, with other users often leveraging tech in unexpected ways.

2

Guaranteeing Privacy and Choice

Users need to be able to actively make informed decisions about their privacy settings. Small red buttons, or phrases like 'advanced settings' can intimidate users, causing them to pick the default settings without necessarily understanding the consequences of that choice. Settings should be simple to understand and easy to configure, and their presentation should not try to influence the user. Include periodic notifications for the user to review configuration that results in data being shared and ensure a diverse user base is considered when establishing default privacy settings.

3

Combating Gaslighting

Gaslighting is when a person manipulates someone psychologically into doubting their memories and judgment. If a user can remove all evidence of an action taking place, or if there never was any evidence, this could lead to someone starting to question their memory. Timely and pertinent notifications as well as auditing are essential for making it obvious who has done what and when. Technology needs to be transparent about where changes have been made and when remote functionality is triggered, making it difficult to obscure or hide gaslighting attempts. Where appropriate, a local override for a remote activation should be provided, empowering users with the ability to choose to retain control of their environment. The user interface and design around such notifications and auditing should be treated with equal importance to that of the regular function of the product, and not assigned to some corner of the interface that is hard to find.

72%

of people seeking help from Refuge last year faced abuse via technology. (SOURCE: REFUGE)

4

Strengthening Security and Data

It is important that products are secure, only collecting and sharing necessary data, thereby limiting the risk that they could be used maliciously. This involves thinking beyond the traditional security threat models and paying attention to the potential risk trajectories if the technology is used to abuse. For example, it is common that many home computer-based devices/services are managed by one user, even though they are used by many members of the family (e.g. virtual assistants, subscription channels, family calendar/data sharing plans, etc.). An intuitive and easy way for family members to subscribe and unsubscribe could be a more effective model, empowering users with joint control.

5

Making Technology More Intuitive

Victims of coercive control live in complex, ever-shifting worlds and may lack the energy or confidence to navigate new technologies. If all end user technology was intuitive to use and understand, this could help reduce the risk of abusers dominating with their greater technical confidence, either with threats or by installing applications the victim doesn't understand. The combination of ease of use and an auditing feedback loop to every user can provide reassurance to a potential victim that they are not being controlled by the technology in question.

While many see coercive control as an issue impacting women, it has wider ramifications in society as it can happen in any type of relationship – especially where there is a power imbalance. Some examples would be between carers and the vulnerable, elderly, or disabled, within institutions and even in the workplace. Our five design principles would equally apply to technologies built for all these situations.

There could be 125 billion internet-connected devices by 2030. As these devices become more prevalent, abusers will have more tools to manipulate their victims. It is critical that we safeguard new technology with strong anti-abuse protections by default so that abusers cannot use these tools to harm victims. Making technology resistant to coercive control ensures that others cannot exploit inventions, tarnish intentions, or dim the light of technological achievement. Most importantly, it is a key step towards making the tech world safer for all of us.

UK Digital Minister Caroline Dinenage:

"Technology brings huge benefits for our lives, whether that is by helping us stay connected or getting groceries delivered to our door.

But we know it can sometimes be misused to exploit vulnerable people. The government is acting to bring in new laws to help make sure smart devices are secure and I am pleased to see IBM taking a lead in this area to help tackle this kind of abuse."

UK Minister for Safeguarding Victoria Atkins:

"Domestic abuse is more than just physical violence, with perpetrators trying to manipulate their victims and control their every move. Technology that was designed to connect us all, can be exploited to cause victims untold misery.

"We are bringing forward the Domestic Abuse Bill - a once in a generation effort to combat this insidious, controlling behaviour. However it will take all of our society to collectively come together and tackle abuse, which is why efforts such as IBM's design principles are an important step in battling this crime."

[1] https://ncadv.org/statistics

[2] https://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures

[3] https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf

[4] https://www.unwomen.org/en/news/stories/2020/3/news-womens-needs-and-leadership-in-covid-19-response

[5] https://news.un.org/en/story/2020/04/1061052

[6] IBM: "Coercive Control Resistant Design: The key to safer technology" (2019) https://www.ibm.com/blogs/policy/wp-content/uploads/2020/05/CoerciveControlResistantDesign.pdf