Coercive Control Resistant Design

The key to safer technology

Adopt a mindful approach to design, ensuring your technology is resistant to being used as a tactic of domestic abuse

Authors
Sarah Burne James
Miriam Franklin
Jessica Evans
Lesley Nuttall

Designer
Amy Magistris

“When we see new technology come out, people often think, ‘Wow, my life is going to be a lot safer". But “we often see the opposite with survivors of domestic violence.”[1]

- Katie Ray-Jones, chief executive of the US National Domestic Violence Hotline

This guide can help developers, designers, architects and anyone else creating new technology, make lives safer by reducing the risk of tech-enabled coercive control.

Table of contents

What is coercive control?

Coercive control creates invisible chains and a sense of fear that pervades all elements of a victim's life[2].

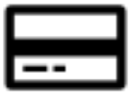
Domestic abuse is all about control. It is a systematic, determined behaviour on the part of the abuser to control the victim.

Historically, responses to domestic abuse have been built on a violence model that equates partner abuse with specific incidents of assault or threat. However, the form of abuse that drives most victims to seek outside assistance is where they have been subjected to a "purposeful pattern of behaviour which takes place over time in order for one individual to exert power, control or coercion over another"[3]. This pattern of domination is known as coercive control. "Violence is used (or not) alongside a range of other tactics – isolation, degradation, mind-games, and the micro-regulation of everyday life (monitoring phone calls, dress, food consumption, social activity etc)."[4]

Coercive control has been recognised as a crime under UK law since legislation came into force in December 2015 in England and Wales, and April 2019 in Scotland[5]. The Government's coercive control literature specifically highlights that technology can be used for abuse[6].

Domestic abusers can use technology more than ever before to control their victims – often by exploiting the tools of everyday life. Abusers gain access to personal and home devices, online accounts and even children's toys and devices. What is particularly insidious is that applications designed with the best of intentions, are being used for malicious purposes. To give you 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 feature can be used to entrap victims, with notifications being sent when an attempt is made to leave the home.



The credit card app that provides instant purchase notifications was built to help combat fraud. However, it's use can give enhanced control over victims with details of their spending being instantly monitored.

Creators of technology are mostly unaware that their technology could be used to abuse someone[7], and even if they are aware their ability to react may be hindered by misconceptions.

This guide is focused specifically on coercive control as we believe this is the area of domestic abuse that is most readily enabled by technology. We would welcome further work exploring other areas of tech-enabled abuse.

Why think about coercive control?

"Research suggests that domestic abuse characterised by patterns of coercive control and/or stalking is more likely to end in homicide" [8]

Domestic abuse is pervasive; the Office for National Statistics estimates that in England and Wales 2 million adults experienced domestic abuse in the year ending March 2018. This equates to approximately 6 in 100 adults[9]. In a study by Refuge[10] more than half of young people said they had experienced controlling behaviour in relationships.

This is a significant issue in society but why do we, as technologists, need to think about coercive control?

Technologists have the opportunity to create products which are designed to prevent coercive control and therefore do not contribute to, or enable, society's problems. If our technology is being used to cause harm we cannot rely on a defence of ignorance. We need to assume that attempts will be made to use our technology for malevolent purposes and do our utmost to design it to be resistant.

Beyond the ethics, there are several business motivations to consider:

Consumers prefer ethical products. In a European study of consumer attitudes, 70% of consumers surveyed mention that social responsibility was important to them when it comes to choosing a product or service.[11]

By improving the usability, security and privacy of your technology (to reduce the risk of abuse) you make it a better experience for your current users and more accessible for a diverse range of new users.

There is a growing risk of reputational damage from technology being used for coercive control.

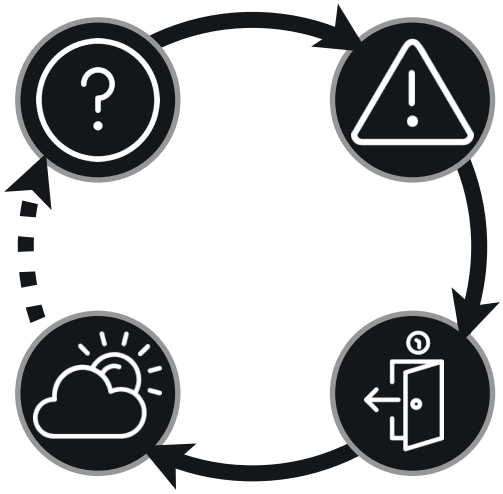
The Lifecycle of abuse

Victims of domestic abuse struggle to leave, and can remain in abusive relationships for many years[12]. Victims are constantly weighing up the risks and consequences of one course of action over another, and many choose to stay for reasons such as lack of alternative accommodation, lack of independent access to money, or the effect leaving may have on their children[13].

There are four distinct states of victim's experiences in an abusive relationship[14]. While not everyone will experience each state, there are distinct needs at each of these stages.

1. Unaware
Experiencing abuse but yet to fully identify this as coercive control

2. Aware
Recognising that a partner is abusive, but not yet making any decisions about what to do next and may not intend to end the relationship



3. Leaving
Deciding to end the relationship and working out the best way to do this, including thinking about alternative living arrangements

4. Recovering
Has ended the relationship and is focussing on the future. May still be in contact with their abuser, fearful of further harm, considering returning to their ex-partner or potentially at risk of entering into another abusive relationship

Figure 1: Four distinct stages experienced by those in an abusive relationship

The most dangerous time for victims is when they leave the relationship; this is often the time when abusers escalate physical violence, or resort to physical violence for the first time[15].

When a victim uninstalls the devices, this can escalate a conflict, experts said. "The abuser can see it's disabled, and that may trigger enhanced violence"[16].

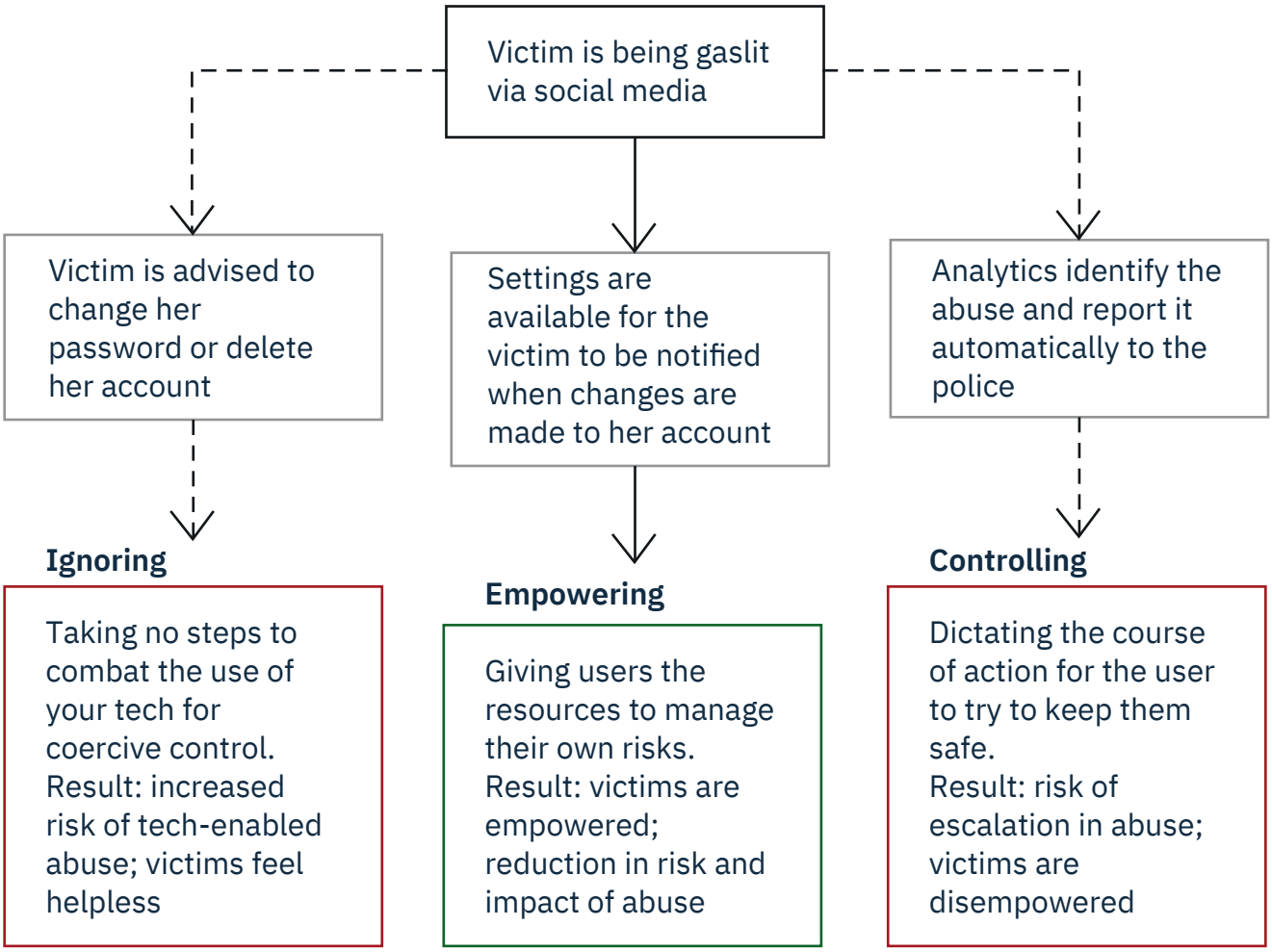
As technologists we need to understand that within our user base there will be people experiencing all four stages of abuse. A successful solution works for the victim whilst in an abusive relationship – allowing them to manage their risk throughout.

Telling someone in stage 1 that "You can contact our support team for help if you are being abused" is unproductive as the victim is not yet aware they're being abused and won't reach out for help.

Someone in stage 4 may have blocked their abuser's number, but if they are still alerted when a blocked number tries to make contact this can invoke a continued level of stress and fear

What kind of response is most helpful?

We are able to act, but as technologists we mustn't be tempted to cast ourselves in the role of "saviour". If victims aren't allowed to make their own decisions, they are simply being moved to another form of control[17]. It's important to find the correct level of response – not ignoring or controlling, but simply empowering victims.



Ending domestic abuse is not simple; coercive-control resistant design is about many subtle decisions that need to be made. To aid in making these decisions, later in this guide we will go through the five key focus areas that our research has identified as being key to designing technology that is resistant to abuse.

Using this guide

If you are a developer, designer, architect or simply making new technology then this guide is for you. There are resources to support victims of tech abuse, but no guide we could find for technologists to avoid contributing to the problem - so we made one!

Abusers are inventive, and technology is constantly evolving – there isn't an exhaustive list of coercive control situations to refer to. The answers will be different for each new technology, and you'll have to weigh up potential risk vs reward for your users. This guide will help you and your team learn about coercive control and how it could apply in your work; walking you through key topics to consider during your design and development process.

We recommend that your whole team read the guide then spend some time together to discuss it; you can use the checklist in each section to start things off. You and your team's ideas can influence design decisions, highlight changes you want to make or gaps where you need to research further. This guide is just the beginning – you know your technology and your business best, and you should tailor your discussions to suit your users' needs.

Five key themes

This section outlines the key areas to consider when developing coercive control resistant technology; including an explanation, worked examples, and checklists for readers to reflect upon. The examples themselves are fictional but draw on our research and discussions with victims and experts of domestic violence to ensure that they are realistic.

The five key themes are:

Diversity

Recognise a diverse user base and have a diverse development team.

Privacy and Choice

Empower users to easily make active and informed decisions about their privacy settings.

Security and Data

Build secure technology, and only collect necessary data, limiting the risk that data from your product can be used maliciously.

Gaslighting

Disrupt attempts at manipulating someone into doubting their memories and judgement with pertinent, timely notifications and auditing.

Technical Ability

Ensure use of your technology is intuitive and can be understood by all, regardless of their technical confidence.

Diversity

Recognising a diverse user base and having a diverse development and design team are key to designing technology that is safe for all to use.

"Mary has escaped her abusive husband Dave to a refuge with her young children, Toby and Stacey, and has hidden her location data on all her apps. When Toby's dad messages him asking for a photo of his homework Toby doesn't think anything of it and sends it to his dad. Toby doesn't realise the photo has location data embedded in it. Dave uses this to find the refuge and waits outside to threaten Mary. Terrified, she has to scramble to find somewhere new she can safely stay with her children".

The creators of this app used personas to discover use cases, but the personas didn't include children. The team, therefore, didn't come to appreciate that children would not understand the terminology used in their privacy conditions. This led to Toby sharing his location data unknowingly, which is then used by Dave with harmful consequences.

"Jessica asks Sue to set up a smart speaker in her house because she doesn't know how to work it, so Sue creates the credentials and connects both their phones. A few months later, after the relationship becomes abusive, Jessica gets a restraining order against Sue so she can't come to the house. However, Sue is still logged into the speaker and uses it to play threatening messages to Jessica. As Jessica doesn't know how to remove Sue's access, she has to suffer this intrusion in her home or stop using the speakers"

By making assumptions that adults are completely in control of their devices, we may be ignoring the fact that devices are often shared.
At any point in time, a set of login details may become unwanted
and we should strive to make it
simple for users to regain control of their devices and manage credentials effectively.

"We need to add depth to the pool from which tech is born, for everyone's benefit"[18]

Designing technology for yourself is simple; you know your needs, what outcomes you are trying to achieve and what makes the best user journey for you. But it's important to remember that you alone cannot represent all users. Each person will likely have different needs and may utilise your technology in unexpected ways potentially resulting in unintended consequences.

"One family had to flee the entire district, as the perpetrator located them due to the victim's son becoming 'friends' with another boy on [social media] who had his location linked to his name."[19]

Currently user profiles are still too limited and miss key issues that subsets of the user-base are facing[20]. Furthermore, the user research is sometimes not actually used to influence key decisions or is misunderstood by the development team. Considering a range of user profiles and choosing a diverse design and development team with a variety of experiences will allow you to uncover a more complete set of requirements and identify a wider range of potential issues.

Designers and developers have a level of responsibility to protect any users, even if they are not the main target audience. Understandably there is a trade-off between the cost of programming a possible scenario versus the probability of a scenario occurring. However, by including the impact of the scenario occurring in your decision-making you may decide that a high-probability, low-impact scenario is just as important as a low-probability, high-impact scenario in protecting your users. This third variable of 'impact' is key in identifying your Stress Cases and your vulnerable demographics.

Diversity discussion checklist

We are considering a diverse user base.

We have a diverse development team.

We are including user profiles that are not our initial target market.

We are exploring the unhappy paths.

We are assessing the impact of edge cases and the consequences/ impact if they occur.

We are ensuring that our decisions are being influenced by diverse data.

Privacy and choice

We need to empower users to easily make active and informed decisions about their privacy settings.

“Louise is setting her social media privacy settings: the choices are a big, green 'accept default' button and a smaller 'advanced settings' button. Louise chooses the 'accept default' option as it's easier and more appealing.
Later that day she accepts a friend request from a male acquaintance, and this is unknowingly posted to her profile page based on the default settings. Louise's abusive husband sees this update and decides to punish Louise.”

By making custom Privacy settings less appealing to users with a smaller button, and more daunting by using the word 'advanced', the app is encouraging people to choose the default settings. They may then be unaware of the settings they have chosen. It is important to encourage users to make an active and informed decision about their privacy settings.

"Alex has a shared shopping account with his abusive partner Lana. He goes on to secretly buy himself some new clothes while Lana is out of the house. After payment, the app sends a push notification to all users, without warning, about the purchase. Alex had completely forgotten that this setting was switched on. Following this, Lana restricts Alex's access to money for the next week."

Although Alex had chosen his privacy settings at some point in the past, he did not remember his choices. If the app had reminded Alex that each user would be notified before he completed the purchase or provided regular reminders to Alex on who is set-up to receive shared notifications, he may have chosen to abort or to change his settings before proceeding.

“I had a hard time convincing [the police] the solution wasn’t just to delete my [app] account. What happens online does have very real consequences and it does need to be taken as seriously. [...] Too many young people get told “block their profile” “come off social media” and I don’t think that’s an answer." [21]

Account privacy and data security have been hot topics in recent years. Since the changes introduced with GDPR[22], developers have been working to improve the level of privacy users can invoke; however, all this hard work improving user control is wasted if the users themselves aren't aware of this functionality or don't understand how to utilise it.

Victims of coercive control can suffer stress-related exhaustion which in turn can lead to cognitive impairment[23]; it can cause them to behave irrationally and unpredictably, be confused and forgetful. Victims and those who support them need their technology to be transparent and clear regarding what information is shared and recorded so they can use it with confidence. The settings should be simple to understand and easy to configure and their presentation shouldn't try to influence the user; ensuring users can make active and informed decisions.

> ***The survivor didn't know how to turn off the notification to the other party about whether it's read or not . . . [the abuser] would go on a rant like, "I know you read this, I know you saw it" . . . which prompted more harassment."[24]***

Fearing the risk that someone else may have changed the settings or that the victim did not understand the consequences of their choices, you can create warnings or information before a user is about to take an action. Similarly, providing regular notifications for privacy configuration that results in data being shared to outside individuals or organisations ensures the user continues to make the right choices for them.

In the circumstance where the user has not chosen their privacy settings, the default settings for your software are of huge importance. The appropriate settings will be different for each technology, and you may decide it appropriate to differ these based on demographic also (e.g. tighter privacy settings for under 18s). Remember to consider your diverse user base when deciding these settings and do not choose these based on the happy path alone.

Privacy and choice discussion checklist

Our tech allows users to make informed choices before making updates.

Our users are clear about who will be informed of their actions and who can view their data.

Our users continue to be sent regular notifications for privacy configuration that results in data being shared.

Our users can amend their privacy settings clearly and easily.

We have assessed what are the most appropriate default privacy settings are for our tech.

We are supporting users to make intentional choices about their privacy settings.

Security and data

Building secure technology, and only collecting necessary data, limits the risk that data from your product can be used for coercive control.

"Maria's phone battery has started draining really fast, but she doesn't realise that this is because her boyfriend Jose has installed spyware on it. He took the opportunity to install it when she let him use her phone to look for directions on their last date, because he said his data was running low. Jose can now see every keystroke Maria makes on her phone, monitor her location and more."

Having no clear indication from the phone of what is draining the battery, or no nudge from the apps she uses that something else is running in the background means that Maria doesn't spot the spyware

Giving Maria an indication that her phone may have spyware running would allow her to make prudent decisions about how to use her phone now that she knows she is under surveillance

---

"Lin was reluctant to share her email password with Roger, but he insisted, saying it was important to have trust when you are in a relationship. Now Roger is able to access many of Lin's accounts linked to that email address. Lin doesn't know that her navigation app is saving a history of everywhere she goes. This is linked to her email account, so Roger now has access to this too."

If Lin's apps had encouraged her to enable two-factor authentication, Roger would have an additional barrier. It would be harder to access all of Lin's accounts without her knowing, even though he has her password.

Security questions as the second factor would not be enough, as people's partners and families will often know the answers to the questions.

"Full access to someone's phone is essentially full access to someone's mind"[25]

Spyware[26] is surveillance software that is used by abusers to spy on their victims, often installed on the victims' mobile phones. This can give the abuser access to the location, messages and other activity the user carries out on the device. According to Kaspersky Labs, over 58,000 Android users had spyware installed on their phones in 2018[27]. Attempts to highlight the presence of spyware ensures the user is making informed choices.

It is not just spyware, however, that presents a danger. Applications that are designed for legitimate purposes, such as anti-theft, anti-fraud, friend locator, emergency response, parental control apps or others, can be leveraged to spy on and control victims. Many victims are unaware that these 'dual-use' apps can be manipulated in such a way. This lack of awareness creates confusion and adds to the omnipresence of the abuser.

"A number of clients have informed me their location had been tracked by a GPS track finder application and they receive threatening and intimidating messages from the perpetrator saying 'they know where they are and to look out'."[28]

Perpetrators of coercive control who use technology maliciously are often authenticated users of applications, with regular privileges, or have demanded passwords and access to devices. They utilise standard functionality for their aims. This type of persona is generally outside the standard security threat model. Furthermore, with the increase in the use of 'one account' to login to multiple sites and services, abusers could have access to data from multiple sources – with just one password.

Hacks or data leaks into the public domain risk data being discovered by the abuser. Any time you are collecting data that you don't need, you are exposing your users to potential risks, with no discernible benefit. Through the lens of coercive control, however, this risk is increased. Victims of coercive control are placed at much greater harm if information about them is made available, as abusers may use it to track them down, or to exert further control. We are not proposing that no data should be collected, but data collection, sharing and storage should be considered pragmatically in view of the potential risks. Privacy by design is a requirement of GDPR, so we need to design for privacy as well as security[29].

Security and data discussion checklist

Our technology has features to protect against actively malicious apps

Our technology will tell the user if it detects evidence of spyware

We have assessed risk versus value for the data we will collect

We have considered threat models for authenticated users that intend to use our tech's functionality for abuse

We have considered harms that could result from data we control being leaked or hacked

We have considered harms that could result from the data we share with other services and apps

Our users are clear on what data they are sharing with us

Gaslighting

Pertinent, timely notifications as well as auditing are key to disrupting attempts at manipulating someone psychologically into doubting their memories and judgement.

“Rob is at home and turns the heating up to 22 degrees. His partner, Angus, can control the heating remotely from his phone and turns the temperature back down to 17 degrees. This is a continuous pattern throughout the afternoon. Rob is uncomfortably cold and starts to question whether he really remembers altering the heating himself or if he imagined it.”

Having no clear indication on the heating device as to what changes have been made, leaves Rob in the dark and causes him to question himself. If the interface provided information about who/what/when last changed the temperature, Rob would be able to understand what was happening.

Furthermore, having a manual override on the device to allow Rob to limit what changes are being made would return some of the power and reduce his discomfort.

"Julie messages John and asks if she can spend the day with her friends. John replies to the message and says this is fine.

While Julie is out, John deletes the messages from the chat and when Julie returns, he confronts her about where she has been. Julie searches for the messages as proof that they had agreed she could go but the messages are no longer there. John convinces Julie that she imagined the conversation."

Giving John the ability to delete messages without a trace allows him to alter 'the truth' and causes Julie to question her memory of what really happened. If an app wants to include functionality like this, it should at least be obvious to other users that a change has been made.

“If you tell the wrong person your husband knows your every move, and he knows what you’ve said in your bedroom, you can start to look crazy,” she said. “It’s so much easier to believe someone’s crazy than to believe all these things are happening.” [30]

Gaslighting is all about gaining control over a victim by making them believe things that are not true and question themselves[31]. It is done slowly, so the victim doesn't realise how much they've been brainwashed. Technology can play a key part in this, especially when it can be accessed or controlled by more than one user or can be accessed remotely.

Abusers use apps on their smartphones, which are connected to the internet-enabled devices, to remotely control everyday objects in the home. They can do things like modify the thermostat temperature, lock/unlock doors, change the wifi password, adjust the volume on speakers or have phantom door bell callers. When these incidents are repeated time and time again, it can be deeply destabilising.

If one user is able to change the history or "truth" without other users knowing, they are able to portray a false series of events. If your settings allow users to make changes on a shared account / device without the other users being notified this creates a knowledge imbalance across the platform.

> ***"They'll hack into their phones and they'll hack into their accounts. Especially with intimate partner victimization . . . oftentimes these people share and know what is very personal information . . . because that was not something that they necessarily kept private when the relationship was a trusting, loving, good one."***[32]

Often, people in romantic relationships will share passwords[33] and the security questions set on their accounts will refer to easily discoverable information (e.g. date of birth or mother's maiden name), granting the abuser practically free reign. Furthermore, it could be fairly easy for the abuser to gain access to their victim's phone and add their own credentials for future access. It is important that the victim still has a way of identifying where changes have been made even if the regular notifications would not apply here.

Keeping all users up-to-date with changes and activities may seem like a contradiction to the Privacy/Choice section, where the victim wishes to keep their information private; so, again, instead of making what you think is the best decision for your users, you should aim to empower the user to make the decisions for themselves so they are aware of how the software will react to their actions and what will or will not be shared with themselves and others.

Gaslighting discussion checklist

- We do not allow one user to change the "truth" or history
- Our technology clearly shows when changes have been made to records
- Existing users are notified when new users are granted access to shared devices/services
- All users are notified when changes have been made or actions taken to shared devices/services
- Technology that lets people take control remotely provides a manual/ local override and notifications

Technical ability

It is important that all users of a technology can intuitively use and understand a solution, regardless of their technical confidence.

“Sinead has left her partner Yusuf and is staying with friends. Yusuf warns her not to tell anyone that he has hit her, threatening that he will hack into her social media accounts if she does. He shows he is serious by sending Sinead her IP address, telling her this is proof that he is able to do it.”

Sinead doesn’t know what an IP address is, but she believes Yusuf is capable of hacking her accounts. He doesn’t actually know how to do this, but he can use this threat as a means of control.

If the social media site had clear help available for users worried about being hacked, Sinead could gain reassurance in this scenario.

“Olivia is on maternity leave, caring for her newborn son, so she is currently spending a lot of time at home. Her controlling father has recently installed a connected doorbell, so every time it rings, he gets a video to his phone. Olivia doesn’t know how the doorbell works; she isn’t sure if it is recording all the time. So, she is nervous about leaving the house or having her friends come to visit without his permission.”

The doorbell device’s security features require an application be installed in order to be operated. If it is complicated to set-up and use, or even if it is presented to be so, it could be a barrier to Olivia controlling her own environment.

Marketing the device to a range of users and conducting thorough usability testing will help avoid making users too intimidated to use devices set up by other adults in their home.

"They don't have to actually do the work. They don't have to compromise any accounts" ... "They just have to make the victim worried about what they might do next.”[34]

Victims of coercive control live in a complex, shifting world where their abuser exerts control not just over their actions, but also often of their understanding of reality. It is cognitively taxing for victims to navigate this world, and to be constantly evaluating the risk involved in various actions, and how to keep safe[35]. Under these circumstances, many victims may lack time, cognitive energy or confidence to navigate complex technologies.

Less than half of victims knew how to change some of their security settings and over 20% had their partner set-up their phone for them[36].

Since the advent of the personal computer, technology has frequently been marketed towards men, and it is widely reported that men are much more comfortable tinkering with technology[37]. This is just one illustration of a potential exclusion of a whole demographic of people. When looked at in the context of coercive control, it becomes clear that it is a cause of great potential harm. For example, connected home solutions are often installed, operated and understood by a single user who is more confident with technology[38]. If a victim of abuse cannot intuitively use a technology, such as to control the lighting in their own home, it is facilitating more control to be ceded to the abuser.

Even minor changes, such as wording could make a difference to a user's experience here. One idea is to simply reword an “Advanced Settings” button to “More Options”, meaning a less confident user is more likely to click and therefore have access to the functionality.

Technical confidence has also been weaponised by some abusers, who use the threat of hacking their victims’ accounts as a way to keep them quiet[39]; even if they have no intention or method of actually carrying this out.

Technical ability discussion checklist

We have done usability testing with a diverse user base

Users can learn to use the technology without the need for “tinkering”

We have considered if focus on our target demographic could cause exclusion, risk or harm

We have avoided wording such as “advanced settings” that may discourage some users

Our product is marketed in a way which makes it approachable to beginner users

Closing

"Not only is coercive control the most common context in which [victims] are abused, it is also the most dangerous"[40]

Technology is increasingly a part of our daily lives. It streamlines our work, eases our routines and enriches our experiences. While new technologies can bring immense benefits in a domestic situation, they can also be exploited by abusers to exert an unprecedented level of control over their victims.

We are a team of technologists working for IBM, in various roles. While we are experts in technology, we are not specialists in domestic abuse or coercive control. Through our research it has become clear to us how prevalent tech-facilitated coercive control is. In fact, a survey of domestic violence support workers found an almost complete overlap between technology abuse and domestic abuse with 98% saying they had clients who had experienced technology-facilitated abuse[41].

One goal of this paper is to inform the reader of the diverse ways in which technology is being used by abusers to harm their victims. In publishing this information, we are keenly aware that abusers might learn new ways to abuse. However, as technology-facilitated abuse is already extremely prevalent, we believe it is better to share this knowledge and encourage technology which resists coercive control.

"What we've seen time and time again is that perpetrators tend to be one step ahead in leveraging technology to use it as a tool for abuse"[42]

In our constantly changing and growing world of technology, it is projected that there will be 64 billion internet-connected devices by 2025[43]. As connected devices became more prevalent, this will provide a wider array of 'tools' for abusers to use against their victims. Perpetrators of coercive control are creative, and with the evolving nature of technology we would welcome further research in this area to ensure our understanding remains current.

Using the knowledge gained from this paper, start asking the questions, open up conversations and adopt a mindful approach to design. It is not enough just to think about making our systems more profitable, faster or feature rich, we must work to ensure our technology is resistant to being used for harm.

Deprive abusers of the ability to use technology against their victims.

Diversity

- [ ] We are considering a diverse user base.
- [ ] We have a diverse development team.
- [ ] We are including user profiles that are not our initial target market.
- [ ] We are exploring the unhappy paths.
- [ ] We are assessing the impact of edge cases and the consequences/impact if they occur.
- [ ] We are ensuring that our decisions are being influenced by diverse data.

Privacy and choice

- [ ] Our tech allows users to make informed choices before making updates.
- [ ] Our users are clear about who will be informed of their actions and who can view their data.
- [ ] Our users continue to be sent regular notifications for privacy configuration that results in data being shared.
- [ ] Our users can amend their privacy settings clearly and easily.
- [ ] We have assessed what are the most appropriate default privacy settings are for our tech.
- [ ] We are supporting users to make intentional choices about their privacy settings.

Security and data

- [ ] Our technology has features to protect against actively malicious apps
- [ ] Our technology will tell the user if it detects evidence of spyware
- [ ] We have assessed risk versus value for the data we will collect
- [ ] We have considered threat models for authenticated users that intend to use our tech's functionality for abuse
- [ ] We have considered harms that could result from data we control being leaked or hacked
- [ ] We have considered harms that could result from the data we share with other services and apps
- [ ] Our users are clear on what data they are sharing with us

Gaslighting

- [ ] We do not allow one user to change the "truth" or history
- [ ] Our technology clearly shows when changes have been made to records
- [ ] Existing users are notified when new users are granted access to shared devices/services
- [ ] All users are notified when changes have been made or actions taken to shared devices/services
- [ ] Technology that lets people take control remotely provides a manual/local override and notifications

Technical ability

- [ ] We have done usability testing with a diverse user base
- [ ] Users can learn to use the technology without the need for "tinkering"
- [ ] We have considered if focus on our target demographic could cause exclusion, risk or harm
- [ ] We have avoided wording such as "advanced settings" that may discourage some users
- [ ] Our product is marketed in a way which makes it approachable to beginner users

Other resources

If you or someone you know is experiencing domestic abuse, there are organisations available to support you. Some are listed below.

For IBM employess, the **Employee Assistance Programme (EAP)** offers confidential counselling and legal advice.

For the UK:

National Domestic Violence Helpline for women sufferers or those calling on their behalf

Men's Advice Line for male sufferers

Broken Rainbow UK for lesbian, gay, bisexual and transgender sufferers

Respect Phoneline for perpetrators who want to stop

References

[1]Bowles N, June 2018, The New York Times - Thermostats, Locks and Lights: Digital Tools of Domestic Abuse

[2]Women's Aid - What is coercive control?

[3]Home Office, December 2015, Controlling or Coercive Behaviour in an Intimate or Family Relationship: Statutory Guidance Framework

[4]Cedar Network - What is coercive control?

[5]Coercive control has not yet become an offence in Northern Ireland but is likely to be implemented soon - BBC News - Domestic abuse bill: Coercive control to become offence in Northern Ireland

[6]Home Office, December 2015, Controlling or Coercive Behaviour in an Intimate or Family Relationship: Statutory Guidance Framework , Types of evidence

[7]Women's Aid - How common is domestic abuse?

[8]Dr Monckton Smith, 2019, Intimate Partner Femicide: using Foucauldian analysis to track an eight stage relationship progression to homicide

[9]Office for National Statistics, November 2018, Domestic abuse in England and Wales: year ending March 2018

[10]Refuge, March 2017, More than half of young people experiencing controlling behaviour in relationships

[11]J Singh, O Iglesias, J. Manel, December 2012, Journal of Business Ethics - Does Having an Ethical Brand Matter? The Influence of Consumer Perceived Ethicality on Trust, Affect and Loyalty

[12]SafeLives - How long do people live with domestic abuse, and when do they get help to stop it?

[13]Davies J, Lyon E, Monti-Catania D, 1998, Safety Planning with Battered Women – Complex Lives/ Difficult Choices, Ch.3-Ch.5.

[14]SafeLives - Tech vs Abuse p.13

[15]Davies J, Lyon E, Monti-Catania D, 1998, Safety Planning with Battered Women – Complex Lives/ Difficult Choices; Women's Aid - Why don't women leave abusive relationships?

[16]Bowles N, June 2018, The New York Times - Thermostats, Locks and Lights: Digital Tools of Domestic Abuse

[17]Davies J, Lyon E, Monti-Catania D, 1998, Safety Planning with Battered Women – Complex Lives/ Difficult Choices, Schecter study quoted on p.13

[18]Winning L, March 2018, Forbes - It's time to prioritize diversity across tech

[19]Woodlock A, 2013, SmartSafe - Technology-facilitated stalking: findings and resources from the SmartSafe project

[20]Novinson M, September 2018, CRN - Security Decisions Are Different When Women Are In The Room

[21]An activist and campaigner from Bristol, who experienced abuse as a young teenager.

[22] EU GDPR.ORG

[23] Jonsdottir IH, Nordlund A, Ellbin S, Ljung T, Glise K, Währborg P, Wallin A, March 2013, Cognitive impairment in patients with stress-related exhaustion

[24] Freed D, Palmer J, Minchala D, Levy K, Ristenpart T, Dell N, April 2018, "A Stalker's Paradise":How Intimate Partner Abusers Exploit Technology

[25] Eva Galperin, security researcher, Electronic Frontier Foundation.

[26] Norton UK - What is Spyware?

[27] Cimpanu C, April 2019, ZDNet - Over 58,000 Android users had stalkerware installed on their phones last year

[28] Woodlock D, November 2015, DVRCV Advocate Autumn/Winter 2015 - Remote Control

[29] IBM Secure Engineering Framework

[30] Ruth Patrick, who runs WomenSV, a domestic violence program in Silicon Valley. Bowles N, June 2018, The New York Times - Thermostats, Locks and Lights: Digital Tools of Domestic Abuse

[31] The National Domestic Violence Hotline- What is gaslighting?

[32] Woodlock D, November 2015, DVRCV Advocate Autumn/Winter 2015 - Remote Control

[33] April 2018, CBC - How one woman is helping others overcome "hacking abuse"

[34] Novinson M, September 2018, CRN - Security Decisions Are Different When Women Are In The Room

[35] Brewster S, (1997). To be an Anchor in the Storm: A Guide for Families and Friends of Abused Women.

[36] Woodlock D, 2013, SmartSafe - Technology-facilitated stalking: findings and resources from the SmartSafe project

[37] Damour L, November 2009, Education Week - Teaching Girls to Tinker

[38] Naughton J, July 2018, The Guardian - The internet of things has opened up a new frontier of domestic abuse

[39] Novinson M, September 2018, CRN - Security Decisions Are Different When Women Are In The Room

[40] Evan Stark, 2007, Coercive Control. How Men Entrap Women in Personal Life. New York: Oxford University Press

[41] WESNET The Women's Services Network, Recharge: Women's Technology Safety

[42] Roxanne Leitão, PhD candidate at Central Saint Martins. Braithwaite P, July 2018, - Wired - Smart home tech is being turned into a tool for domestic abuse

[43] Newman P, January 2019, Business Insider - IoT Report: How Internet of Things technology growth is reaching mainstream companies and consumers