Abertay University

School of Design and Informatics

An Investigation into Technical Countermeasures Against Smart Home Technology-Facilitated Abuse

Kayleigh Skye Gall

BSc (Hons) Ethical Hacking, 2021

Abertay University
Dundee, United Kingdom

Word Count: 10,885

Table of Contents

Table of Figures

Table of Tables

Acknowledgements

I would like to thank my project supervisor, Dr Ian Ferguson, for the continued guidance and reassurance during this project.

I would also like to thank my parents for their endless support and encouragement through the entire process. And Aidan, who looked after me so well. I couldn't have achieved this without you.

Finally, I wish to acknowledge the bravery of survivors of domestic abuse, their ability to live through and overcome their abuse is a truly astounding feat of strength.

Abstract

Hand-in-hand with the rise of use of smart home technology in homes has come the exploitation of features of smart home devices to facilitate acts of domestic abuse. Perpetrators take advantage of the presumed trust used by the smart home system to harass, control, gaslight, and monitor their victims.
Smart home technology-facilitated abuse is a relatively unexplored area as of yet. Most existing research into prevention focuses on increasing awareness and resources within support services, as opposed to addressing the technical vulnerabilities in smart home devices which facilitate the abuse, and how to secure the technology.

This project aims to explore the possibility of technical countermeasures to technology-facilitated abuse which can be integrated into smart home systems' framework design.

Research into reported cases of 'tech abuse' facilitated by smart home devices and previous work into the subject was used to identify specific methods of abuse and the technical features of smart home devices which are exploited. With this knowledge, requirements of smart home systems to prevent these particular methods of abuse were specified. Using this specification, technical countermeasures to smart home tech abuse were produced, and a framework which implements these anti-abuse countermeasures was designed.
A prototype smart home control application which visualises the user experience of interacting with this system framework was developed in Android Studio.

Produced was a list of design elements which acted as countermeasures against specific methods of abuse which included harassment, gaslighting, stalking, and asserting omnipresence. The countermeasures involved applying existing design elements with an anti-abuse focus, and implementing new features, such as machine learning to identify abusive behaviour within the smart home.
The prototype Android application effectively visualised most of the design elements which were outlined in the framework.

The use of applications of artificial intelligence to identify patterns of abusive behaviour in smart home systems was explored and discussed, and the possible methods to be used were theorised using comparisons to intrusion detection systems.
The financial and legal implications of implementing countermeasures to smart home technology-facilitated abuse was also investigated, considering profitability, consumer relationships, and product safety legislation.

The results of this study provide a feasible step towards further research and development into technical countermeasures to smart home technology-facilitated abuse.

Abbreviations, Symbols and Notation

IoT	Internet of Things
ML	Machine Learning
IDS	Intrusion Detection System
HIDS	Host-based intrusion detection system
AI	Artificial Intelligence
ID	Identification

1. Introduction

1.1 Background

“Internet of Things” (IoT) technology is used in the automation of ‘smart homes’ to allow remote control of devices within the home. Whether it’s controlling the heating, turning on the lights, answering the door, or playing music; IoT technology can make these everyday tasks effortless, and give more control to the user by connecting their home appliances to the internet and allowing commands to be sent to them from the user’s smartphone.
Although smart home device vendors may promise users an improved quality of life and more control of their surroundings with their products, in some cases these same devices are being used to strip people of control of their life and put their safety at risk.

While the number of smart home devices in the world experiences a sharp rise, so do the cases in which these devices are used much more harmfully than their developers intended. 'Technology-facilitated abuse' or 'tech abuse' are terms coined to describe the use of internet connected devices to carry out acts of domestic abuse and intimate partner violence. In 2019, UK domestic violence charity Refuge reported that 72% of women who accessed support through their services had experienced some form of tech abuse.

The ability to control a wide range of devices throughout the home completely remotely opens up a whole new world of disturbing opportunities for an abuser. Whereas in the past tech abuse has been confined to persistent phone calls or online slander on social media, advances in IoT technology and growth of use of smart home tech allow abusers to harass, control, and monitor their victims with ease.
The abuser's remote control over a victim's physical surroundings using smart home devices in their home can be used to assert and perpetuate a sense of omnipresence in the victim's life. This assertion may be coupled with gaslighting and intimidation tactics to make a victim compliant in their abuse and harassment via these smart home devices. Due to a lack of awareness of technology-facilitated abuse, victims are often not informed of the signs that they are being abused this way, and commonly do not realise that they are being abused for quite some time.

Tech abuse is not something that only very technically skilled people can do. Numerous studies have found that many of the methods used to carry out technology-facilitated abuse do not require a high level of technical ability. This puts a larger amount of people at risk from technology-facilitated abuse.

Within the current body of previous work, the majority of solutions and countermeasures to technology-facilitated abuse have been rooted in raising awareness and providing training and facilities to support services. There is little acknowledgment of the requirement of technical countermeasures to tech abuse designed and implemented by IoT and smart home device vendors to protect their consumers.
Assumed trust between smart home members is common in smart home systems. It is a clear sign of the lack of diverse users which have been considered during usability testing and often leads to lacking security measures which are harmful to victims.

1.2 Project Overview

This project will explore how technical countermeasures to smart home technology-facilitated abuse can be designed and implemented into the devices themselves to prevent their misuse to carry out tech abuse, and protect victims of this abuse should it arise.

This project aims to identify the vulnerabilities of smart home technology which are exploited to facilitate abuse and produce a series of proposed countermeasures to these specific methods of abuse incorporated into a smart home system framework.

This aim will be achieved by:

- reviewing previous work on the subject to identify methods of abuse used by perpetrators and the technical features of the smart home devices which are exploited to do this
- specifying requirements of smart home systems to prevent abuse which address the particular methods of abuse identified
- designing a framework of countermeasures to be implemented in smart home systems
- developing a prototype application which effectively visualises the countermeasures and design features outlined in the framework
- discussing in depth the proposed use of applications of artificial intelligence to identify patterns of abusive behaviour as one of the countermeasures designed
- discussing the real-world feasibility of implementing these countermeasures on a large scale, addressing financial and legal implications

The underlying purpose of this project is to call to action technologists to take steps towards creating a safer technology landscape for those who are at risk of technology-facilitated domestic abuse.

2. Literature Review

Smart home and IoT technology-facilitated abuse is a modern-day issue which requires modern-day solutions. As smart home systems and IoT devices have become more commonplace in the average home, cases of technology-facilitated abuse have risen and, in turn, there has been an increase in research into technology-facilitated abuse. Work on the subject spans many fields – informatics, law, social studies – and usually focuses on the objective of finding solutions and countermeasures to this abuse.

This section covers existing research into the methods and devices used in technology-facilitated abuse, as well as research on both social and technical countermeasures/solutions, before outlining the issues and space for improvement brought up in this research into solutions.

2.1 Methods of Abuse

A research paper by Delaine Woodlock with the Domestic Violence Resource Centre Victoria (2017), introduces the concept of smart home technology being used to convey omnipresence; a technique used in abuse in which abusers assert "a sense of being ever present in the victim's life". Woodlock discusses how mobile and smart technology allows an abuser to be omnipresent in a victim's life beyond what has previously been possible; the constant connection to the victim's home via smart devices breaks down the sense of safety that physical separation originally gave.
Smart home devices exist to replace a wide range of normal items. Publications from BBC (Silva, S. & Franco, T., 2020) and NY Times (Bowles, N., 2018) have reported a range of devices used as tools of domestic abuse: smart cameras, digital locks, and climate control systems.

The risk of falling victim to tech abuse is not only present in co-habiting relationships. Julia Slupska (2019) explains that technology-facilitated abuse can often increase once a victim no longer co-habits with their abuser. This is because the abuser loses physical access to the victim and turns to using technology to carry out the abuse.

Freed et al. (2018) found that the methods used by perpetrators of technology-facilitated abuse could be categorised into one of four areas: exploiting ownership of devices, compromising accounts and devices, sending harassment through online messages/posts, exposing private information.
Where the latter two methods of abuse generally have the result of harassing and/or endangering the victim, and mainly utilise social media to do this, the exploitation of ownership and compromise of devices and accounts can give a high level of control over the victim to the abuser, and has relevance when discussing smart home technology-facilitated abuse.
The research found that this control over the victim's interaction with technology is exploited by both physically and digitally restricting the victims actions and use of technology, monitoring the victim's activities (both physical movements and device usage), and accessing the victim's private information.

The survey data collected by Freed et al. comes from victims of all kinds of domestic abuse. Alshehri et al. (2020) outline the clear differences between traditional abuse, tech-abuse and "Smart HOme facilitated Tech-abuse (SHOT)". Where generic tech-abuse is abuse which surrounds online information or devices, SHOT is abuse altering the victim's environment by using technology –

described as ‘effective, efficient, and untraceable methods to carry out stalking, gaslighting, and other abusive actions’ (p. 2).

2.2 The Abuser

Slupska (2019) outlines the threat model of technology-facilitated intimate partner violence, stating the abuser is highly motivated, but is not necessarily highly technically skilled. Abusers are obsessed with intimidating and controlling their victims and will use a variety of methods to do this – ranging from technologically simple, to sophisticated.
As mentioned in Slupska’s paper, technology facilitated abuse does not usually require a high level of technical skill. This is reiterated in the Tech vs. Abuse report, which states that abuse facilitated by internet connected devices is no longer something which only a ‘tech-savvy’ perpetrator can carry out.

Freed et al. (2018) concluded that “most of” the attacks which were found through their research were technologically very simple and did not require advanced computing skills to carry out.
Analysis from this study found that abusers made no attempt to escalate privileges or use forensic tools, as they were in the position where they had authenticated-level access to the victims’ devices – whether gained through physical/mental/emotional coercion or trust. These abusers were referred to as “UI-bound”, as they only used functionality available through the user interface.

2.3 Existing Research into Solutions

The Gender and IoT research team at University College London has produced a large amount of research into the use of IoT products for technology-facilitated abuse, or “tech abuse”.

Key findings published in *Safe – The Domestic Abuse Quarterly* stated that support services suffer a lack of ability to advise on tech abuse, due to limited resources to increase awareness and technical capacity to aid victims of IoT tech abuse (Lopez-Neira et al., 2019).
The paper goes on to make recommendations to support services, tech vendors, and policy officials. These cover the need for more resources provided to support services, as well as input from cybersecurity practitioners to enable service workers to help victims of tech abuse and incorporate tech abuse in risk assessments. Also recommended is consideration of tech abuse in legislation.

These recommendations are mirrored in the *Tech vs. Abuse Research Findings*, which states that there is “a strong demand for training and support” to be given to support service workers in regards to how to support victims of tech abuse (Think Social Tech, Snook, & SafeLives, 2019).

2.4 Issue with Victim-Focused Solutions

One of the main issues with many research findings which offer solutions and countermeasures to technology-facilitated abuse, is that the recommendations made focus primarily on either technical measures to be taken by victims to protect themselves from attempts at tech abuse, or on increasing awareness and support service practitioner training to help those who have already been a victim of technology-facilitated abuse. These ‘solutions’ put responsibility onto victims to prevent their abuse, and support workers to help victims after the abuse has already taken place.

In a BBC article (2020), IBM Security Expert Lesley Nuttal, explains that “the burden of safety” should not fall onto the user, but instead should be shifted towards thoughtful designs. Nuttal et al. (2019) calls for action from technologists, stating “if our technology is being used to cause harm we cannot rely on a defence of ignorance.”.

In *Safe at Home: Towards a Feminist Critique of Cybersecurity* (2019), Julia Slupska writes of how diverse design teams are crucial to ensure that the product developed appeals to a wide audience, rather than solely reflecting the needs and desires of those with lives which are akin to that of the design team.
This paper also explains that abuse victims struggle to leave their abuser for a number of reasons including threats and intimidation tactics, and social and economic dependency on their abuser. Furthermore, the abuse victims are at the highest risk of violence and death when they try to leave their abuser.

A paper from University of Florida (Silva, M. & Oliveira, D., 2021) explores how existing advice for victims of technology abuse can be harmful to Brazilian favela women. Favelas are informal settlements in Brazil with no governmental regulation, developed as a result of lack of affordable housing. Due to the low income levels and lack of social connections out with the favela communities, escaping abuse can be economically impossible and socially isolating. Furthermore, police are not welcome, nor necessarily trusted, in these communities.
Although this study was specific to Brazillian favelas, these circumstances are not unique, and reflect other communities. Of the 1.32 million domestic abuse-related incidents and crimes reported to police in England and Wales in 2019, 57% were considered criminal offences by police, of these cases only 11% led to prosecutions: 6% of all the reports (Office for National Statistics, 2019).

Distrust of the police is amongst many reasons that victims may be reluctant or unable to seek help. A survey carried out by Domestic Violence Resource Centre Victoria (Woodlock, 2017) found that 85% of the women who didn’t seek help when suffering from technology-facilitated abuse admitted that they were “too embarrassed to seek assistance”.

2.5 Research into Technical Countermeasures

Although there is a lack of existing technical countermeasures to technology-facilitated abuse, some previous work in surrounding areas offer possible solutions and relevant insights.

Islam et al. (2016) from the American International University of Bangladesh proposed a smart home device as a technical countermeasure to domestic abuse. *HomeGuard* is a smart home system designed for emergency response for victims of domestic violence. Although this device is targeted at ‘traditional’ domestic abuse, it introduces the use of artificial intelligence to combat domestic violence. The proposed device records a message spoken by the victim and uses natural language processing to analyse the message and determine the best plan of action, based on a library of contact details for police, lawyers, support services, and hospitals.

A research paper published by USENIX (Zeng, E. & Roesner, F., 2019), explores the design of smart home systems in regards to security and privacy in the context of a multi-user smart home. The research found three types of conflict which can arise from multi-user smart homes: power and access imbalances, privacy

violations, and direct conflict between users over shared devices. A prototype app – *SmarterHome* – for controlling a smart home system was created and tested in a voluntary user study.
The results of the user study found that many of the specific security and privacy functions of the *SmarterHome* app went unused by the test users, and instead respectful usage was guided by social norms rather than software features. The results stressed the importance of high trust relationships, existing positive norms in the home, and good communication between members of the home to result in conflict free usage.
In a presentation of the study at the Usenix Security Symposium (USENIX, 2019), Zeng discussed how the access controls made available by *SmarterHome* were misused. He recounts how one of the test users gave her husband child-level access controls since he was prone to "messing up the configuration". Although that was a consensual decision in this instance, it highlights how easily functionality specifically designed to make smart home systems more safe and secure can be abused to possibly take control away from a victim.

Alshehri et al. (2020) produced a number of technical measures that could be implemented in smart home systems to prevent tech abuse – each listed with its specific objective and possible downsides.
Solutions included having devices distinguish users through voice recognition to protect users' data from other users, though this is specific to voice assistants and runs the risk of the devices becoming less controllable. Another solution involved providing emergency access to support services in case of abuse, this reflects the ideas explored with *HomeGuard* as in both cases the device would make decisions on behalf of the users to contact support or emergency services - though devices taking decisive action like this is usually considered bad practice.

The study contained conflicting solutions surrounding the permanence of usage history. This highlights the issue of usage history having both positive and negative effects in terms of technology-facilitated abuse. The research solutions by Alshehri et al. propose that deleting usage history periodically could protect the victim by hiding their escape plans, however this may help abusers gaslight their victims and cover up their abuse. On the contrary, making all usage history permanent would hold abusers accountable for their actions, and allow victims to collect evidence, but means that proof of victims' escape plans or contact with support services may be found by the abuser.

A research paper from IBM (Nuttal et al., 2019) explores coercive control resistant design, and provides checklists for technologists to follow throughout the development and testing process to ensure that their technology is resistant to misuse in domestic abuse.
The key areas identified in the paper are Diversity, Privacy and Choice, Security and Data, Combatting Gaslighting, and Technical Ability. The checklists provided suggest a range of solutions such as encouraging users to make use of two-factor authentication and make informed decisions about their privacy settings, providing notifications to users about devices usage, and including user profiles which do not fit the initial target market in testing.

2.6 Use of Artificial Intelligence

Artificial intelligence (AI) is a powerful tool which has found uses in many areas of modern society, from customer service to cancer research. Machine learning is a type of artificial intelligence that focuses on computer systems learning from experience to improve algorithms for analysing data to make decisions.

Recently, machine learning has been explored as a tool to help stop forms of abuse. A proof of concept for the use of machine learning in analysing cases of domestic abuse was run in Spanish police departments in partnership with SAS Institute (2020). The system used data collected from victim interviews, police reports, and other resources to calculate a 'recurrence risk' score which allowed a relevant protection and vigilance plan to be put in place – ensuring the correct and appropriate resources are assigned in each situation.

Machine Learning has also been explored as a tool to recognise abusive behaviour. Research from the Bracket Foundation (2019) explores the use of artificial intelligence to prevent, detect, and prosecute perpetrators of online sexual abuse of children. The use of computer vision, natural language and voice, and predictive AI are discussed regarding their possible ability to "improve on [predictions] offered by traditional analytics technology".

3. Methodology

This section provides detail of the three-stage process of designing a smart home application framework which integrates countermeasures to technology-facilitated abuse and developing a simple prototype for visualisation purposes.
The stages are requirement specification, framework design, and prototype development. This includes designing countermeasures to fit the requirements which are developed based upon the specific methods of abuse used, then visualising how some of these countermeasures would be integrated into a smart home control application by building a prototype.

3.1 Specifying Design Feature Requirements for a Secure Smart Home System

Through reviewing previous work and existing reports of technology-facilitated abuse, several methods used by perpetrators of technology-facilitated abuse were found. These methods take advantage of the access to smart home devices and their features in order to gaslight, harass, and monitor their partners.

3.1.1 Gaslighting

In the 1938 stage play “Gas Light” (Hamilton, 1938), a husband slowly convinces his wife that she is going insane after she notices the gaslights in their home dimming for seemingly no reason, when in actual fact he is sneaking into the upper floors of their home and lighting the gaslights there, causing the lights where his wife is to dim.
This behaviour is mirrored by abusers who use smart home technology to alter their victims' surroundings such as playing music, adjusting the temperature, or turning other IoT devices on/off without the victim's knowledge (Bowles, 2018). This may be followed up by 'gaslighting' their victims by convincing them they are seeing and hearing things which are not real or losing patches of memory.

This method of abuse is made possible by the lack of easy access to device usage history for users, allowing abusers to control the devices secretly.
To combat gaslighting, a smart home system must provide evidence of *which users* have sent *what commands* to *which devices* at *what time*. This would prevent abusers from convincing their partners that certain changes to the smart home system were or were not made, as the evidence provided by the smart home system would contradict any false claims by the abusers.

Providing evidence of all past or recent commands sent on the smart home system would require usage history to be captured, logged and stored permanently. In the context of an abusive relationship, this may have some negative effects. The issue surrounding usage history permanence is as follows: making all smart home device usage history permanent and readily available to users to view combats gaslighting and helps victims uncover abuse and collect evidence against their abusers, however it also allows abusers to track all usage activity by the victim, which may add to their sense of omnipresence and control or even allow them to uncover the victim's escape plans. Making usage history erasable or regularly wiped presents the inverse issues.

3.1.2 Omnipresence

Concerns over usage history permanence in an abusive context are often due to the issue of proof of the victim’s access to domestic abuse support services being accessible to the abuser. The sense of omnipresence asserted by the abuser can

take advantage of the victim's lack of technical understanding and make them believe that their abuser will know everything they do online.

To combat the omnipresence asserted by abusers, safe and secure access to support materials, along with reassurance that the browsing history is not recoverable must be provided to victims.
To provide this private and secure access to support materials to victims without fear of their abuser uncovering evidence of their search and browsing history, access to these materials should be offered with encrypted, cache-free, history-free browsing. Although most browsers have private browsing sessions readily available to users, due to the nature of their abuse, some victim of technology-facilitated abuse may be lacking technical confidence to be able to access a private browsing session or the effects of their partner's asserted omnipresence may make them too cautious of negative repercussions should their abuser uncover their attempts to access support.
Safe access to support materials addresses the issue of history permanence by providing a secure place to browse support materials without history being saved and made available to users.

Although a log of smart home command history may still have negative consequences by allowing an abuser to monitor their partner's activities, which may be used to further assert a sense of omnipresence in their life, access to the same information is easily accessible to the victim. The log of commands is accessible to all household members and will be clear, accessible, and jargon-free. This allows victims to understand what information their partner can see and how they are accessing it.

There is not a clear universal solution for this issue which would benefit every domestic abuse victim. Further research into the area involving input from survivors of technology-facilitated abuse is necessary to understand the intricacies of the issue and develop an effective solution.

3.1.3 Harassment

One reported method of abuse is relevant in relationships where the abuser and the survivor are no longer cohabitating, but the abuser can still gain access to the smart home devices in the survivor's home. It is also relevant to cohabiting couples where the abuser often leaves the home for extended periods of time whilst the victim stays.

In this instance, the abuser uses the smart home devices in the victim's home to monitor them (Hammersley, 2018), or to harass them by altering their surroundings (Ghebreslassie, 2018). This may leave victims lacking the technical skill or virtual access to the devices required to change their state, trapped in their home in sweltering temperatures or with loud music playing.

This method of abuse is made possible by the remote access to smart home devices even when out of the home. Some smart home control applications require connection to the same local network in order to access and control the devices on that network, but others will allow remote control from anywhere.

To combat this method of abuse users who are in the home should take priority over those who are accessing the devices remotely from another location.
One method of implementing this is providing manual controls on the physical smart devices which are able to override commands sent from mobile devices.

The ability to turn off or disable the devices is not sufficient, as a victim doing so may “trigger enhanced violence” (Bowles, 2018). IBM outlines manual override on smart devices as a design principle which combats gaslighting (Nuttal et al., 2019). It also combats harassment and stalking inside the home.

3.1.4 Stalking and Monitoring

Some abusers use smart home devices to stalk and monitor their partners when they are in the home. There have been several reported cases of abusers using devices such as video doorbells, wall-mounted tablet cameras, and home security cameras to watch and listen to their victims remotely. These types of devices are readily available from tech vendors such as Amazon, Arlo, Google and more.

As smart home monitoring devices such as security cameras are often built to be discreet, as to blend in with home décor, these devices may be hidden from victims. Furthermore, victims may not be aware of all features of multi-function devices like home hubs - which may have built in cameras and/or microphones which could be used to monitor the home remotely.

Indicators of device state would provide users with more awareness of the user of devices within their home. This should involve both virtual indicators, like on the smart home mobile application, and physical hardware indicators on the device themselves. Multiple indicative lights on smart home devices can be used to show device state and device access state, so that members of the smart home are aware when the device is on and when the device is being accessed.

3.1.5 Summary of Requirements

All of the requirements discussed above are represented in the table below, with the corresponding method of abuse and technical feature of the smart device which facilitates the abuse.

Method of Abuse	Technology that facilitates abuse	Requirement
Gaslighting	Remote control of devices with lack of evidence of who has accessed them.	Provide evidence of *which users* have sent *what commands* to *which devices* at *what time*.
Harassment	Remote control of smart home devices from out with the home	Users within the home must take priority over the devices which alter the environment over users out of the home.
Omnipresence	Technology that the victim doesn’t understand can be used to assert omnipresence	Provide safe and secure access to abuse support services and materials to potential victims
Stalking/Monitoring	Video and audio recording equipment can be hidden in the home and accessed remotely or secretly.	Provide indicators of device state and device access state on the smart home control application and on the device itself

Table 1 - Requirements of smart home systems based on methods of abuse

Not all cases of technology-facilitated abuse are the same, and so solutions which benefit some victims may make others' situations worse. Previous work has proved it difficult to create one framework which is beneficial to all types of domestic abuse victims or prevents all types of domestic abuse perpetrators. This highlights the need for research in the field to find solid universal technical solutions which don't put any victims at more of a risk than they were without.

Despite the complications with technical countermeasures to technology-facilitated abuse, technologists and smart home tech vendors should still put in the effort to make moves towards implementing safe and effective countermeasures. A study into the unintended harm of cybersecurity countermeasures found that cybersecurity countermeasures may have several damaging effects such as displacement of harm, amplification of harm, or disruption of other countermeasures (Chua et al., 2020). These should be considered when taking steps to make countermeasures to tech abuse.

3.2 Designing a Secure Smart Home Control Application Framework

Using the requirements specified in the previous section, a series of countermeasures were designed, along with a framework of a smart home control application which incorporates these countermeasures.
Smart home control applications are a common control method for smart home devices. They allow users to access and control their devices remotely from a smartphone or tablet.
Some of the countermeasures outlined in the previous section are applied to physical smart home devices, so cannot be visualised via the smart home application framework.

The framework design is loosely based on the *Google Home* app which is a mobile app used to control *Google Nest* devices.

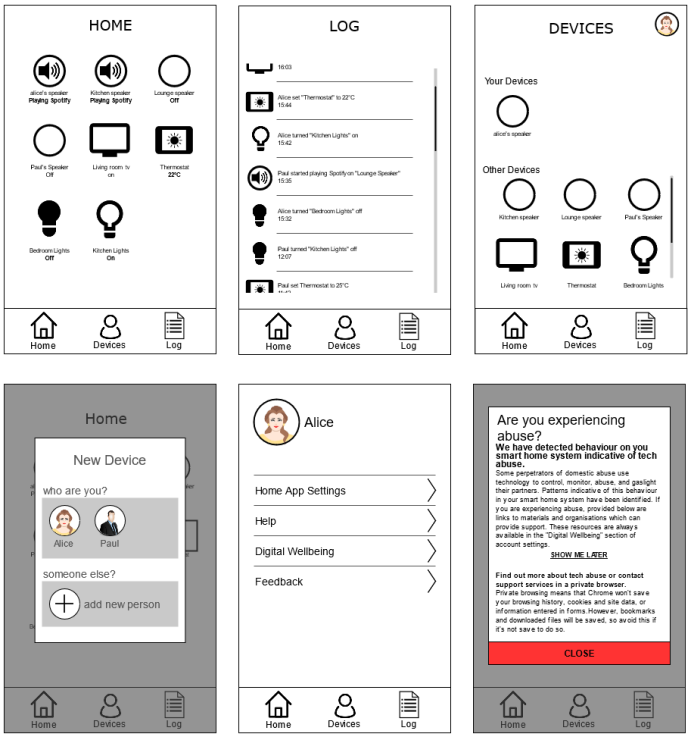

Figure 1 – Secure smart home system control application framework design

The application framework design features a navigation bar on the bottom of the screen which provides quick and easy access to the applications three main pages: the home page, the usage log, the device list. Through the device lists page, there is access to an account menu page which provides further access to settings and help pages.
The framework design incorporates countermeasures, based on the requirements formed in the previous section, to combat gaslighting, harassment, omnipresence, and stalking.

3.2.1 Device List

The Home page displays a table of all the devices currently set up on the home network. An icon for each device is displayed above the device name.
The current state of each device is displayed on this home screen in text below the device name and further indicated by a change in the device icon to reflect the device's actions. This provides indication to users of what devices are active in the home and how they are being used, in order to prevent gaslighting and stalking.

3.2.2 Log

The solution includes a Log page which provides a history of all device usage activity to all users. The intent of this is to combat gaslighting and uncover abuse by allowing the victim to easily view the activity throughout their home. The Log is one of the three pages accessible from the bottom navigation bar. This makes it simple to access; taking just one step, instead of several more complex steps which may dissuade a less technically confident user.

The Log works using a system which distinguishes members of the household by using separate user accounts tied to specific devices. When setting up a new smart home device, each current member of the household can be declared. Then every new device on the home network which attempts to interact with the smart home devices thereafter must identify itself via the smart home control application as one of these users or a new person. This identity is used within the log when documenting all interactions with smart home devices in the home.

Each entry in the Log will list the device that is being interacted with, the command sent to the device, and person/account that is sending the command. The symbol for the device will be displayed at the start of each log entry to better convey the information in an easier to digest format - not just blocks of text.

The Log targets two types of abusive situations: the situation in which, within a co-habiting couple, the abuser remotely alters the devices around the home, then lies to the victim about it, convincing them to doubt their perceptions and memories; the situation in which a victim may have left their abuser, but the abuser still has remote access to the smart home devices in the victim's home and uses this to monitor and abuse the victim. The way in which the Log helps in these situations is that it serves as proof of who has been accessing and controlling the smart home devices.

A potential risk that is posed by the Log is that if a controlling partner can monitor all interactions their victim has with remote devices in their home, even when they are not present, then this works to solidify the sense of omnipresence that the abuser may hold in the victim's eyes. Furthermore, if an abuser is controlling to the point where they don't allow their partner to use the devices without permission (for example, the victim is not allowed to change the temperature

setting, or not allowed to go into certain rooms), then this takes away the victim's ability to secretly use/interact with these devices.
In the case of this study, the intention of the Log is to work alongside other components to assist victims in realising that they are being abused and prevent gaslighting. The presumption that users in a scenario where an abuser scolds their partner heavily when they use the smart devices in their home, are more likely to be aware that they are being abused than those who are being manipulated into doubting their own perception.

3.2.3 Pop-Up

The solution proposes the use of applications of artificial intelligence to analyse the usage data being sent to the log to detect abusive use of the smart home devices on the network. The user identities will be used to distinguish members of the household, and AI methods such as machine learning will analyse how their interactions with the smart devices in their home conveys the nature of their relationship.
Should an instance of technology-facilitated abuse be identified, a notification from the smart home control application will be sent to the identified victim of the abuse on their smart device/s and the next time the application is opened on a device which has been identified as belonging to the victim, a pop-up message will appear with information about tech abuse, and links to support services.

As is featured on most domestic abuse support service websites, a large, clear exit button will be always available within the pop-up window (Refuge, 2021). This considers victims who may be in close proximity to their abuser when the pop-up appears, allowing them the ability to escape the window very quickly.
After the first section of text is a "Show me later" button. This considers victims who may have time to read part of the pop-up message, and be interested in finding out more, but aren't in a safe environment to do so immediately. This option causes the pop up to appear when opening the application again after a set amount of time has passed. This time could be anywhere between 2 and 24 hours – research is required into how to best identify a time when the victim is apart from their abuser.

Many considerations were made regarding the language used on the pop-up, as domestic abuse is a sensitive topic which should be approached carefully and respectfully.
The information on the pop-up takes a three-tiered approach; with consecutive passages of text increasing in length and decreasing in size to capture the reader’s attention and draw them in gradually. This is to avoid the pop-up being immediately disregarded by users who may benefit from it.

The large message at the top of the pop-up is "Are you experiencing abuse?". This appears in large and bold text.
The message is phrased as a question instead of a statement like "You are being abused.". This is done with the intention to not be harsh or forceful, which may cause victims who are having a difficult time coming to terms with their abuse to push back on accepting help. The use of a question is also made so that the pop-up is initially more engaging to the user.
The question used de-personalises the abuse, as opposed to a question like “Are you being abused?”. This is done to avoid the message being interpreted as a personal criticism, by instead removing the abuse from the victim and treating it as something which is separate from them.

The simplistic language of the question, free of any technical jargon, such as 'algorithms', 'patterns', 'system', or 'machine learning', considers victims who are not as technically confident and may be intimidated by this kind of language. More natural language is used to make the interaction more human, and more comforting and inviting to the victim.

Below the first title, it a subtitle which is smaller than the title, but also in bold text. This text adds context by giving a very brief explanation as to why the user is seeing this pop-up message. This message contains slightly more complex language to explain that potentially abusive behaviour has been identified but does not contain any jargon as to keep the entire message easy to understand.

Below the first two sections of text, the pop-up contains information outlining what technology-abuse is. It uses simple, non-technical language to explain how various forms of technology abuse can manifest, making use of keywords such as “control’ and “gaslight” which may stand out to a victim of these methods of abuse.

An option on the pop-up will offer the victim the ability to open support materials in a private browser, with an explanation outlining that the browsing history is not saved on a private session. Although private browsing sessions are always available using many web browsers, a victim who is less technically confident may not be aware of them, or still worry that their abuser may find their browser history. This option considers the history permanence problem, by allowing the victim a safe channel to research abuse and contact support services to plan their escape, in which history is not saved, and so will not be accessible by the abuser.

3.3 Developing a Prototype Application

A prototype application which visualises the user experience of several of the features of the countermeasure framework was built in Android Studio. Throughout development, the application was tested using a Pixel 3 API 29 Android Virtual Device.
Fragments were used for the three main pages (Home, Devices, Log) to allow a consistent navigation bar to be visible at the bottom of the screen, granting quick and easy access for the user to these three key pages.

3.3.1 User Identification

User identity is initially declared by the user the first time that the smart home control application is opened on a new device.
SharedPreferences are a feature of Android which allows local storage for small amounts of data. SharedPreferences are used to store the user ID as a string which can be accessed by activities and fragments throughout the application to dynamically display the user ID and make decisions based on which user account is identified.
An initialisation function is called every time the application starts which checks the SharedPreferences for the user ID. If a user ID string is not found, a pop-up activity is displayed which prompts the user to pick from any of the previously declared users, or to identify themselves as a new user.

3.3.2 Log

The Log interface features a *LinearLayout* nested within a *NestedScrollView*, which acts as the list of commands. The *NestedScrollView* allows many commands to be loaded into the Log without escaping the bounds of the screen.

As to keep the prototype self-contained and not require internet connectivity to demonstrate its features, a list of pre-configured commands is stored in an Android resource file which is accessed from the Log fragment.
Each command in the resource file is stored as a separate string value, which contains the user ID of the user sending the command, the device name, the device type, the command, and an indicator of abusive behaviour. In a full working solution, each command may contain more features as meta-data, such as location. When accessed by the Log fragment, the list of commands is stored as a string array type variable.

A ‘test’ button was added to the Log page for prototype demonstration purposes. This button triggers a simulation of a command being sent to a smart home device on the network.
When the ‘test’ button is pressed, the next command in the list, which is identified using a global integer variable which acts as a counter, is split up into its individual components. The device name, user ID and command are displayed in the log, and the device type is used to select the correct symbol to display in the log entry. Each new log entry is dynamically added to the top of the *LinearLayout*.

3.3.3 Machine Learning Simulation

The use of machine learning to analyse commands and identify patterns of abusive behaviour was simulated very simply by adding an "X" or "Y" to the end of each command. For the purposes of the prototype, "X" is considered indicative of a normal behaviour, and "Y" as showing signs of abuse.

Whenever a new command is added to the log, the user ID and abuse indicator value is sent to a public interface which can be accessed by a function in the Main activity which analyses each command for abusive behaviour.
To simulate the use of machine learning to recognise patterns of abusive behaviour using the commands sent to smart devices, global integer variables for each user are used as counters which increase every time a potentially abusive command sent by that user is identified. Once a specified number of potentially abusive commands sent from the same user is reached, a pattern of abusive behaviour is identified and a pop-up providing access to support resources will be shown to the identified victim of abuse.

To identify when to send the pop-up message to the victim’s device, SharedPreferences are used to store Boolean values which indicate whether or not an alert is due to show on a specific user's account. Every time the application is opened on a mobile device, the values of the alert Booleans stored in SharedPreferences are checked and if an alert Boolean for the user which is currently logged in is true, then the alert pop up is shown.

In a full working solution, the command analysis may not be run locally, but instead online using a cloud-based solution. This way, the indicator to alert the victim will also be stored online, on the user's account.

3.3.4 Provision of Access to Support Resources

To provide access to support materials an activity which acts as a pop-up window is used. The pop-up style is achieved by dynamically sizing the activity to 90% of the width and height of the host device’s screen size.
To contain all the information required, regardless of screen size, a ScrollView is used in the activity layout. The ‘close’ button sits outside of this view so that scrolling doesn’t move it and it is always present on the screen.

The safe and secure access to support materials is achieved by including buttons in the pop-up activity which open a WebView activity at a specific URL. This allows the user to browse these specific sites in a browser contained within the smart home application.
Several of the WebView's settings are adjusted to not add data to the cache while browsing and to clear history, cache, and form data. These settings allow safe and history-free browsing of the support service websites.

4. Results

The resultant artefacts of this project are a framework of countermeasures and anti-abuse design features for smart home systems designed to combat methods of technology-facilitated abuse, and a corresponding prototype of a smart home application used to interact with the devices in the smart home system.

4.1 Framework Design

The framework includes considerate design features which act as countermeasures to prevent and combat several methods used by perpetrators of technology-facilitated abuse. These include:

- Use of devices to gaslight victim
- Use of devices to harass victim
- Use of control over devices to assert omnipresence
- Covert use of devices to stalk and monitor victim

The table below displays the results of the research and investigation into smart home technology-facilitated abuse, which include the methods used by abusers and the technical features of smart home devices and systems which facilitate this abuse. The table also shows the corresponding requirements to prevent the use of the smart home devices for these abusive acts, and the countermeasures designed based on each requirement.

Method of Abuse	Technology that facilitates abuse	Requirement	Countermeasure
Gaslighting	Remote control of devices with lack of evidence of who has accessed them.	Provide evidence of *which users* have sent *what commands* to *which devices* at *what time*.	Include a Log which lists details of commands sent to smart home devices on the network.
Harassment	Remote control of smart home devices from out with the home	Users within the home must take priority over the devices which alter the environment over users out of the home.	Provide manual override controls on the physical devices within the home, which take priority over remote commands
Omnipresence	Technology that the victim doesn't understand can be used to assert omnipresence	Provide safe and secure access to abuse support services and materials to potential victims	Cache-free browsing of support materials available via "Digital Wellbeing" page
			Machine learning applied to identify possible victims of tech abuse and provide the links to support materials directly.
Stalking / Monitoring	Video and audio equipment can be	Provide indicators of device state and	Smart home device state made

	hidden in the home and accessed remotely or accessed secretly.	device access state on the smart home control application and on the physical device itself.	viewable from the smart home control application.
			Visual/Audio indicators (lights/sounds) on physical devices which change when device is on/off and being accessed/idle.

Table 2 - Countermeasures designed based on requirements to prevent specific methods of abuse

4.2 Application Prototype

The smart home application prototype developed in Android Studio visualises the framework to show the user experience of several of the design features. Included is the user account selection functionality and log used to combat gaslighting and harassment, and a simulation of the use of AI to detect abusive behaviour and provide the victim with access to support services.

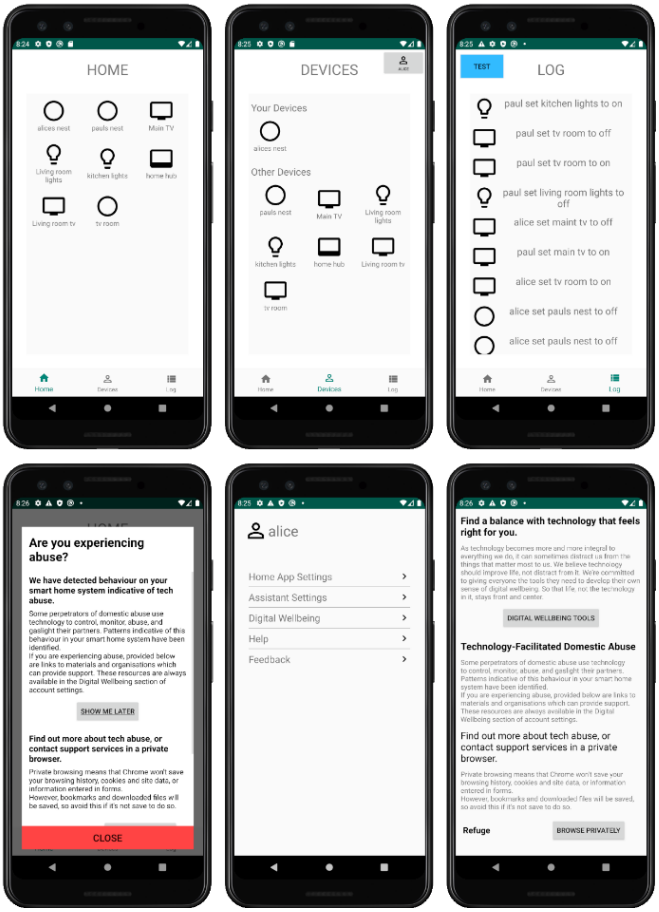

Figure 2 – Prototype smart home control application

4.2.1 Features

The implementation of the Log feature effectively uses strings of commands from an Android resource file and displays them in a scrollable log, which is easily accessible from the home page via the bottom navigation bar. Although the log

doesn’t use real commands being sent on an actual smart home system, the user experience is sufficiently simulated to provide deeper understanding of the concepts put forward in the framework design.

The selection part of the user declaration process is visualised effectively by making use of features of Android to show a pop-up to the user upon first opening the application on a new device. Changes can be seen throughout the application depending on the identified user.

A clear visualisation of the user experience of interacting with the abuse alert pop-up message is given by the prototype application. The simple code which simulates the use of machine learning effectively conveys the idea outlined in the countermeasures framework.

4.2.2 Omissions

There were some countermeasures outlined in the smart home system’s framework which were omitted from the prototype application which was developed. These omissions were made due to time constraints and lack of familiarity with the development environment. The decisions made as to what features of the framework to implement into the prototype were made dependant on how important it was to provide a visualisation for deeper understanding of that feature.

The prototype application effectively allows the user to choose between two pre-set users but does not have the process of setting up a new user account implemented. This feature was omitted as it is a simple concept which is present in many technologies, and so implementing it into the prototype to visualise the user experience is not necessary considering the extra complexity it would add to the prototype to involve local or cloud storage.

The prototype application features a static Home page which lists devices representative of devices currently on the home network. The devices displayed on the Home page do not update to show the current state of the device as outlined in the framework as a method of combatting covert use of devices to facilitate stalking and monitoring of victims. Indication of the current state of smart home devices is a design feature which is very common in smart home control applications, and so it was deemed that visualising this concept to provide better understanding of user experience was not a priority.

Other features which were part of the framework could not be added to the prototype as they were applicable to the physical smart home devices, as opposed to the smart device user interface. These include the audio/visual state indicators on devices, and the manual control override.

5. Discussion

In this section, the conceptual framework design from the previous section will be discussed in further detail. Specific subject areas will be explored, these include the use of artificial intelligence to combat technology-facilitated abuse as outlined in the framework, the financial and legal factors which are relevant to tech abuse countermeasures, and the significance of this project.

5.1 Use of Artificial Intelligence to Combat Technology-Facilitated Abuse

Machine Learning (ML) is an application of artificial intelligence which uses algorithms which learn from previous data and improve without explicit programming. ML is applicable in a wide range of ways, such as recognition, prediction, and monitoring. Applications of machine learning can be found in many different industries including finance, advertising, medicine, healthcare, transportation, manufacturing, and more.

The application of Machine Learning algorithms can be split into two subsections: Classification and Regression. The results of regression algorithms are numerical, and these algorithms are used to predict the value of a dependant variable in relation to an independent variable. Classification algorithms are predictive algorithms which are used to categorise data by using analysis of previous data.

Pattern recognition is an application of artificial intelligence which involves training machine learning algorithms to recognise regularities in data. Pattern recognition, at its core, uses classification to categorise items/events based on previous data. The proposed use of machine learning for detecting patterns of technology-facilitated abuse would apply classification algorithms to analyse logs of commands sent throughout the smart home and categorise the data as either normal or indicative of technology-facilitated abuse.

5.1.1 Comparison to Intrusion Detection Systems

Existing implementations of machine learning being applied to detect adverse behaviour in a network can be seen in intrusion detection systems. Intrusion detection systems (IDS) monitor network traffic for signs of cyber-attack and can use classification algorithms to categorise network packets by the type of attack that may be present. IDS's exist in various forms and can use a variety of techniques for intrusion detection.

Host-based intrusion detection systems are locally installed systems which analyse application logs for signs of suspicious activity. Most HIDS's work using anomaly-detection. Anomaly-detection builds a model of usual traffic and detects possible attacks based on variations from the norm.

Attempts to use a model of non-abusive behaviour in a smart home in an anomaly-based detection solution which is integrated into commercial IoT smart home devices may face some problems. Building a model of usual network traffic for an anomaly-detection system is not 'one-size-fits-all'. Similarly, a universal model of non-abusive smart home behaviour may be impossible or very difficult to achieve. Models of usual network traffic which are used in intrusion detection systems for enterprises are trained using several days (around 7-10) worth of normal traffic on the specific network in which the intrusion detection system will be integrated.

It is impossible to build a model of non-abusive behaviour in each home that a smart home device is set up in (using usage data from the first 1-2 weeks, for example), as there is no certainty that the situation that the device is introduced into is not one that already involves abusive behaviour and imbalanced power dynamics. Haar and Buchmann (2020) write "If the Smart Home network is already compromised when the IDS is put into operation, this state is considered as normal. Thus, there exist situations in which anomaly-detecting IDS cannot increase the network security.", the use of tech abuse detection is comparable to an IDS this way.

Signature-based detection in IDS's uses a pre-configured database of signatures of known cyber-attacks to detect network intrusion. The main drawback of this type of IDS is its inability to detect novel attacks, making it much less effective against zero-days. To combat this issue, machine learning algorithms are often used to improve upon existing anomaly-detection solutions.
Haar and Buchmann (2020) found that signature-based IDS are "better-suited [than anomaly-based detection systems] to secure Smart Homes at the moment" but stress the importance of paying "special attention" to the pre-configured rules used.

Using pre-configured signatures which indicate abusive behaviour for signature-based detection introduces several issues. The first is that abuse involving any patterns or devices which have not been considered in the set, may go completely unnoticed by the detection system. Secondly, a pre-configured solution must be considerate of the variety of contextual situations that a smart home device may be used in - if not, then the pre-configured signatures may put the system at risk of false positives where behaviour that seems harmful on paper is just a by-product of normal use.

5.1.2 Machine Learning Countermeasure Proposal

Abusive Act	Event Sequence	Features Used
Abuser accesses and controls devices when no longer cohabiting with partner	One account continuously accessing and sending commands to devices through a device which is never located in the home.	user account, smart device, device command was sent from, location of smart device, location of device command was sent from
Abuser resets any changes made to device state by partner (either secretly, as part of gaslighting, or blatantly)	One account continuously accessing devices in short succession of another account, and reverting any changes made to the device settings by the previous account	user accounts, smart devices, commands sent, time of commands
Abuser doesn't allow partner to access the devices when the abuser is in the home	All user accounts access smart home devices as normal when the mobile devices connected to the identified abuser's account are out of the home. When the abuser is in the home, only their	user accounts, smart devices, devices commands were sent from, location of smart devices, location of

	account is used to access smart home devices.	devices commands were sent from
Abuser uses devices such as cameras to monitor partner when not in the home	One user account continuously accessing specific devices which provide audio and video from a device which is out of the home, whilst devices connected to another user are in the home.	user accounts, smart devices, devices commands were sent from, location of smart devices, location of devices commands were sent from

Table 3 - Specific abusive acts which may be identifiable by ML

The table above shows a list of abusive acts which may be identifiable by the sequence of events that the smart home system logs, and the features which may be used by a classification algorithm to identify these patterns.
The abusive acts listed in the leftmost column are based on research into descriptions given in reported cases of tech abuse and acknowledge the use of smart home devices to gaslight, harass, control, and stalk victims.

The 'Features Used' column includes the metadata that will be attached to each command sent on the smart home network. Some of this data makes up what is included in the log of commands. Although only some of these features were used in the prototype, in a fuller working solution all of this data may be logged externally to the cloud.
In a cloud-based solution, the pieces of metadata attached to commands can be used as features for classification algorithms which are used to identify abusive behaviour. This identification is made when event sequences which indicate abusive behaviour, as described in the 'Event Sequences' column, are recognised.

Existing research explores the use of machine learning algorithms to recognise behavioural patterns through smart home device usage, with the intention of applying prediction algorithms to improve smart home systems by identifying the user's usual usage patterns.
The use of long short-term memory neural networks to take in usage data and perform classification to identify event sequences is discussed by ElSayed (2020). Neural networks are used in the field of deep learning, to simulate how the human brain processes data. Qolomany et al. (2019) found that automation for 'Smart Buildings' which uses neural networks to recognise sequences based on input from IoT devices is feasible, and provide a deep insight into many technical aspects of applying machine learning in this way.
This project's proposed use of machine learning as a countermeasure to technology-facilitated abuse may use techniques very similar to those explored in these studies, but with an inverse method of recognising adverse behaviour, as oppose to normal usage.

Signs of adverse behaviour and toxic power dynamics in a smart home may be indicative of an abusive relationship and tech abuse. But they may also be symptoms of a harmless power imbalance due to certain members of the household's inability or lack of incentive to use the devices. For any complete solution to be widely integrated into commercially available smart home devices, a large amount of further research and data collection is required, which would require investment from smart home product vendors into the safety of their products for victims of domestic abuse.

Applications of artificial intelligence are already in place on a wide scale to solve a variety of real-world problems; these include banking fraud, network intrusion detection, medical diagnosis, and online abuse. The artificial intelligence market size valued at 27.23 billion USD in 2019 and predicted to reach 266.92 billion by 2027 (Fortune Business Insights, 2020). With the correct investment from smart home technology vendors into the wellbeing of consumers that may be suffering from abuse facilitated by their technology, artificial intelligence in some form may be used to detect signs of this abuse and save lives.

5.2 Financial and Legal Considerations of Technology-Facilitated Abuse Countermeasures

In 2017, Google partially funded the launch of a programme by Refuge to tackle technology-facilitated abuse by training 300 frontline professionals to provide support to victims of this abuse, as well as starting a dedicated expert unit, and running campaigns to raise awareness (Refuge, 2017). This shows that Google is and has been aware of the ever increasing issue of tech abuse for over three years, yet in 2021 their smart home systems still lack levels of security and privacy, allowing any mobile device on the same wireless network as some smart home devices (such as Google Nest or Google Home) to view and control the activity on the device anonymously.
Furthermore, there is no sign that Google has ever implemented any technical countermeasures into their smart home devices with preventing technology-facilitated abuse in mind.

The lack of technical countermeasures and protection against technology-facilitated abuse seen in current smart home systems may be due to the lack of profitability for tech vendors in implementing them.
Due to the nature of domestic abuse, victims are very unlikely to be the deciding party when purchasing a smart home device. Approximately 92% of domestic abusers are male (Office for National Statistics, 2019), and in heterosexual couples, men more often purchase the technology and set it up.

In some cases, abusive behaviour may stem from controlling the smart home devices, with no abusive or controlling behaviour existing in the home prior to the installation of the devices. In these instances, the individual will likely not predict abuse may arise from the smart home device purchase, and so have no reason not to buy it.
Furthermore, due to the lack of awareness of tech abuse within the general public, even if a domestic abuse victim does have the choice of purchasing a smart home device or not, they may not be aware of the risks posed.

The lack of protection for victims of tech abuse does not result in a significant loss of purchase profits for technology vendors.

IBM published several ‘business motivations’ which should be considered by technologists (Nuttal et al., 2019).
The report from IBM suggests that measures taken to reduce the risk of abuse within their products by improving usability, security, and privacy will result in an improved experience for current users. Although this may be true, this may not explicitly drive any new profit, and therefore may not be considered a crucial change.
Furthermore, user experience for some may be impaired as safety features are added. Many smart home systems often work based on presumed trust and respect within a household, increasing security and safety for users could

negatively impact ease of use and setup of the devices for the primary target audience.
The report also discusses how the effects of smart home devices being known to have facilitated abuse may impact consumers' decisions to purchase their products. The reasons for this being that it poses a risk of reputational damage, and consumers prefer ethical products. Although both points are true, there is currently a wide lack of awareness of tech abuse, and so the risk to profitability of smart devices - from either boycotting or consumers choosing to purchase more secure products – is not imminent.

Although pressure from consumers and risk of loss of profit margin are factors which would likely influence technology vendors' decisions regarding safety measures for abuse victims, other means of applying pressure lie in obligation from legislation.

Gender and IoT from UCL has released several reports which address the lack of active legislation surrounding tech abuse, and push for changes to be made by the UK government. In a paper discussing legislation surrounding online harm (2020), they call for statutory duty of care on technology companies to be introduced. This change would hold technology companies responsible for giving users accessible ways to report cases of their technology being used to facilitate abuse and providing more transparent, accessible privacy setting tools. UCL also suggest that technology companies should keep up to date with the tech abuse threat landscape to implement countermeasures accordingly.

Alshehri et al. (2020) suggest a possible solution of adding informative safety labels or leaflets to the smart home device packaging which advises consumers of the capabilities of the device – comparable to nutritional information labels on food products.

In compliance with regulation 13 of The General Product Safety Regulations 2005, many products in the UK include safety warnings advising consumers of possible risks posed by the product – such as choking hazards on children's toys, or safety warnings on kitchen knives. If further research into technology-facilitated abuse can prove that insecure smart home devices pose a risk to domestic abuse victims, then an argument could be made that these devices fall under the requirements of this law, and force technology vendors to disclose the risk. The potential reputational damage and loss of consumer trust that this requirement may result in, may give technology vendors the motivation to implement technical countermeasures against tech abuse into their products.

5.3 Significance

The resulting artefacts of this project provide technical suggestions for countermeasures to combat the use of smart home products to carry out specific methods of technology-facilitated abuse.

The countermeasures were conceived by first acknowledging different specific methods of abuse which are facilitated by smart home devices and breaking down these techniques to pinpoint the technical features of the smart home devices and/or system which allows this. The countermeasures were then designed by addressing the specific technology which facilitates abusive acts and behaviour in the home.

By doing this, the countermeasures are focused specifically on preventing abuse, rather than increasing security of the device and hoping that this hinders an abuser's ability to exploit them.

The framework includes both design features which are not currently heavily prevalent in many smart home systems and design features which are already present in some or most.
A significant part of this project lies with the proposal of existing design elements which are already commonly used in smart home systems and control applications as countermeasures and tools to combat technology-facilitated abuse. These effects of the design elements may not have been previously considered by the development and testing teams.

Due to widespread lack of awareness and understanding of technology-facilitated abuse, it is likely not considered by development teams to any degree of significance throughout designing and testing of smart home devices. Because of this, features of smart home devices which may have a large effect on victims of tech abuse, are deemed inconsequential by developers.

Within existing research, technical countermeasures which focus on and tackle specific methods of abuse are very rare. Where technical countermeasures are discussed in previous work, they are usually mentioned briefly as part of a wider subject area in studies which either look into smart home design for a different purpose (Zeng, E. & Roesner, F., 2019) or discuss all areas of tech abuse, not specifically smart home tech abuse (Nuttal et al., 2019). There is a lack of published concepts for countermeasures against tech abuse which exploits the presumed trust and inadequate safety and security measures which are present in many smart home systems.

This project has brought to light the need for technical smart home technology-facilitated abuse countermeasures and demonstrated how they can be designed taking an anti-abuse focused approach to result in solutions which directly address and prevent specific methods of technology-facilitated abuse.

6. Conclusion

This section discusses the future of research and work into the subject area and summarises the ideas put forward throughout this project.

6.1 Future Work

As discussed throughout this paper, there is a lot of work to be done in technology-facilitated abuse prevention. Large amounts of research and investment are required to build usable effective solutions which can be implemented in consumer products on a widescale.

6.1.1 Prototype

Whilst the Android prototype effectively visualises some of the features of the framework, there were omissions made due to time constraints and lack of technical skill level and familiarity with the software development best practices. Further development of the prototype could be made to implement these features of the framework that were omitted from the current prototype.

Additional work could develop the prototype further using Android Debug Bridge to include network and device connectivity to log and analyse commands being sent to actual smart home devices on a network.
Further communication between fragments and activities along with the use of the Android AnimationDrawable element on the “HOME” page could allow the device icons to visually indicate their current use state.

These improvements would elevate the current prototype to a more visually and technically impressive application, which better encapsulates the theoretical design elements outlined in the framework design.

6.1.2 Increase Awareness and Investment into the Issue

Further awareness of the issue must be raised among technologists, and a level of interest in the effects of these smart home devices be taken by the people and corporations which design and fund them. Raising awareness, however, can only have so much real-world effect; financial and resource investment from technology vendors is required to allow further study and exploration of countermeasures to technology-facilitated abuse.

Further to the financial investment required to develop effective solutions to tech abuse, an emotional investment is required from lawmakers, technologists, and the general public.
Consumer distrust and public criticism can cause great change by putting reputational and financial pressure onto technology companies to address the issues, this may cause them to implement solutions.
Once people care about victims of domestic abuse, then solutions will come about.

Work must be done to continue raising awareness. Once investment is made, further work can be done to investigate the use of machine learning algorithms to identify abuse; this would involve collecting big data and embracing insight from survivors of tech abuse.

Smart home technology development and design teams must be diversified. Diversity within a development team ensures that the insights and life experiences considered throughout the design, development, and testing stages of technology

for the home cover a large range of social, geographical, and economic backgrounds. This varied insight will result in more universal products which are better suited to users from different walks of life.

6.2 Conclusion

The intention of this project was to explore how technical countermeasures can be implemented into commercially available smart home systems and IoT devices against the use of those devices to facilitate domestic abuse and controlling behaviour, and to design a conceptual framework for a smart home system which incorporates countermeasures built to tackle specific methods of abuse.
The framework of anti-abuse design features produced introduces simple measures which can be implemented into smart home system frameworks to prevent misuse in tech abuse. The solutions frame some common design elements in another light to provide understanding of how these elements may be used to prevent an abuser from exploiting the system.

The research and discussion into the use of machine learning classification algorithms provided in this project theorises how future research and work should be able to provide an effective solution to recognise abusive behavioural patterns in smart home systems. This, however, is not a solution which is imminent, due to the need for big data to develop it.

This project provides a step in the right direction; towards further research and awareness of technology-facilitated abuse, and towards the implementation of technical countermeasures to prevent it.
The underlying aim of this project is to act as a push for technologists to take a fresh perspective towards their work, and to consider what changes can be made that would be negligible to the average consumer, but life-changing to vulnerable individuals.

A lot of work still needs to be done, but through considerate design and diverse development, effective steps can be taken to protect victims of domestic abuse from the exploitation of smart home devices to perpetuate their abuse.

List of References

Refuge Charity. (2021). *Refuge Against Domestic Violence - Help for women & children*. [online] Available at: https://www.refuge.org.uk/

Woodlock, D. (2017). The Abuse of Technology in Domestic Violence and Stalking. *Violence Against Women*, Volume 23(5), p. 584–602.

Slupska, J. (2019). Safe at Home: Towards a Feminist Critique of Cybersecurity. *St Antony's International Review*, Volume 15(1), p. 83-100.

Franco, T. & Silva, S. (2020). How smart devices are exploited for domestic abuse. *BBC Click*, [online]. Available at: https://www.bbc.co.uk/news/technology-54554408

Bowles, N. (2018). Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. *The New York Times*, [online]. Available at: https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html

Freed, D., Palmer, J., Minchala, D., Levy, K., Ristenpart, T., Dell, N. (2018). "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*.

Alshehri, A., Salem, M.B., Ding, L. (2020). Are Smart Home Devices Abandoning IPV Victims?. [online]. Available at: https://arxiv.org/pdf/2008.06612.pdf

Lopez-Neira, I., Patel, T., Parkin, S., Danezis, G., & Tanczer, L. (2019). 'Internet of Things': How abuse is getting smarter. *Safe – The Domestic Abuse Quarterly*, Volume 63, p. 22-26.

Think Social Tech, Snook, & SafeLives. (2019). Tech vs Abuse: Research Findings.

Silva, S., Franco, T. (2020). How smart devices are exploited for domestic abuse. *BBC NEWS*, [online] Available at: https://www.bbc.co.uk/news/technology-54554408

Nuttall, L., Evans, J., Franklin, M., James, S.B. (2019). Coercive Control Resistant Design. *IBM Corporation*.

Silva, M. & Oliveira, D. (2021). Brazilian Favela Women: How Your Standard Solutions for Technology Abuse Might Actually Harm Them. *University of Florida*.

Office for National Statistics, 2019. *Domestic abuse and the criminal justice system, England and Wales: November 2019*. [online] p.23. Available at: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/domesticabuseandthecriminaljusticesystemenglandandwales/november2019#prosecution-and-conviction-outcomes

Islam, A., Akter, A., & Hossain, B.A. (2016). HomeGuard: A Smart System to Deal with the Emergency Response of Domestic Violence Victims. *IJCSI International Journal of Computer Science Issues*, Volume 13(6), p. 103-112.

Zeng, E. & Roesner, F. (2019). Understanding and Improving Security and Privacy in Multi-User Smart Homes: A Design Exploration and In-Home User Study. In: *Proceedings of the 28th USENIX Security Symposium*. Santa Clara: USENIX, p. 159-176.

USENIX. (2019). *USENIX Security '19 - Understanding and Improving Security and Privacy in Multi-User*. [video] Available at: https://www.youtube.com/watch?v=EfqHRVSkEUA

Navarro, A., Davies, A. (2020) How Machine Learning Can Help Combat Domestic Violence. *SAS*.

Bracket Foundation, Péron, C., & Macdonald, J. (2019). Artificial Intelligence, Combating Online Sexual Abuse of Children.

Hamilton, P. (1938). *Gas Light*. London.

Hammersley, T. (2018). Jealous businessman spied on ex-partner using iPad mounted to kitchen wall. *Manchester Evening News*, [online] Available at: https://www.manchestereveningnews.co.uk/news/greater-manchester-news/jealous-businessman-spied-ex-partner-14640719

Ghebreslassie, M. (2018). 'Stalked within your own home': Woman says abusive ex used smart home technology against her. *CBC News*, [online] Available at: https://www.cbc.ca/news/science/tech-abuse-domestic-abuse-technology-marketplace-1.4864443

Chua, YT, Parkin, S, Edwards, M, Oliveira, D, Schiffner, S, Tyson, G & Hutchings, A. (2019). Identifying Unintended Harms of Cybersecurity Countermeasures. In: *Proceedings of the Symposium on Electronic Crime Research.* Anti-Phishing Working Group, pp. 1-15.

Haar, C. and Buchmann, E. (2020). Securing Smart Homes using Intrusion Detection Systems. In: *SECUREWARE 2020*. IARIA, pp.46-52.

ElSayed, S. (2020). Machine Learning in Smart Homes. *Medium*. [online] Available at: https://medium.com/swlh/machine-learning-in-smart-homes-5f39e9600cf0

Qolomany, B., Al-Fuqaha, A., Gupta, A., Benhaddou, D., Alwajidi, S., Qadir, J., Fong, A.C. (2019). Leveraging Machine Learning and Big Data for Smart Buildings: A Comprehensive Survey. In: *IEEE Access*, vol. 7, pp. 90316-90356.

Fortune Business Insights. (2020). *Market Research Report*.

Refuge. (2017). New programme to tackle technological abuse. [online] Available at: https://dev.refuge.org.uk/7008-2/

Gender and IoT. (2020). *Futureproofing Online Harms legislation*. Tech Abuse. [online] University College London. Available at:

https://www.ucl.ac.uk/steapp/sites/steapp/files/ucl_g-iot_online_harms_tech_abuse_one_pager_-_feb2020.pdf

The General Product Safety Regulations (SI 2005/1803). Available at: https://www.legislation.gov.uk/uksi/2005/1803/regulation/13/made

Appendices

Appendix A – Framework Design

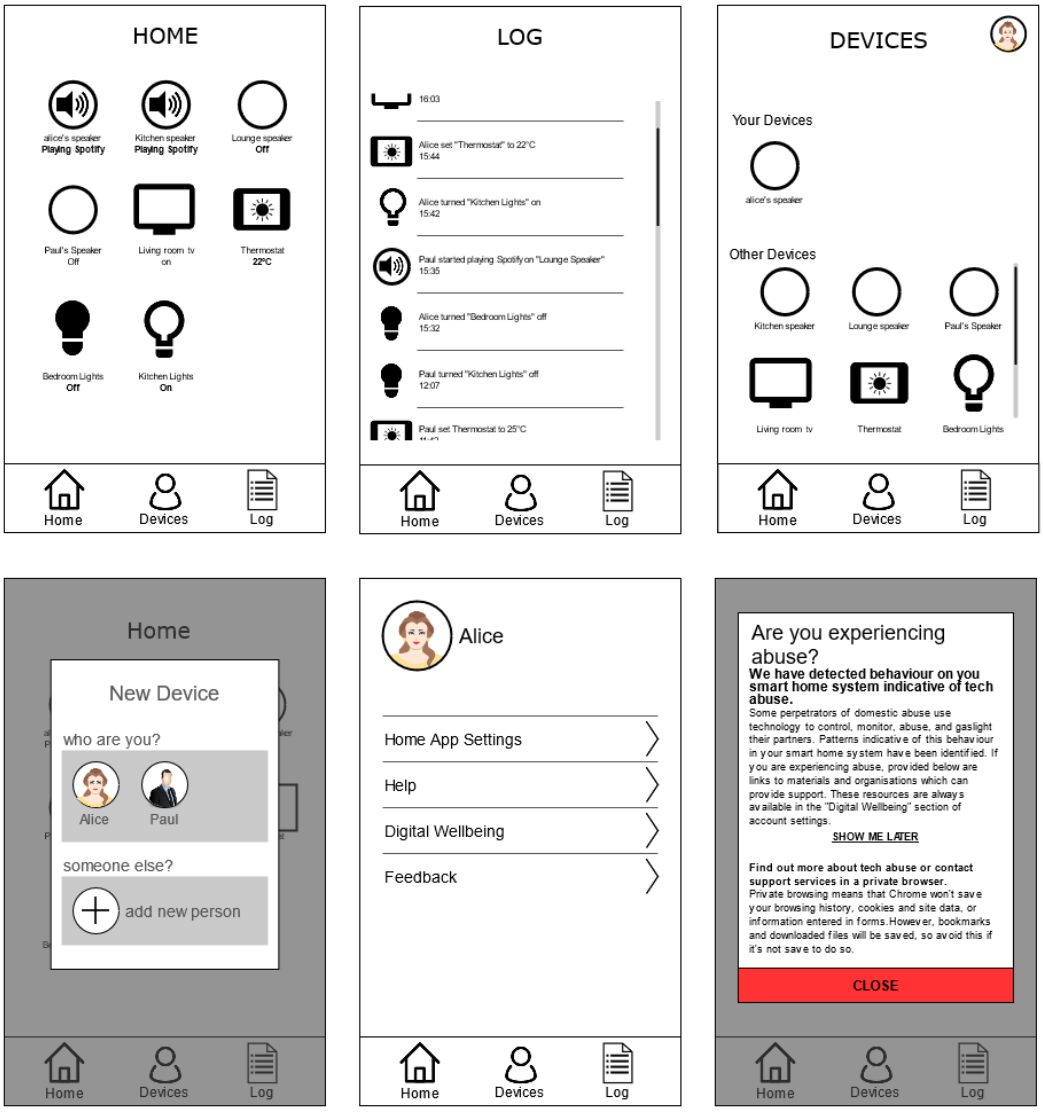

Figure 3 - Initial application framework design

Appendix B – Prototype Application

All prototype application source files can be found at:
https://github.com/alwaysbiue/honsproj

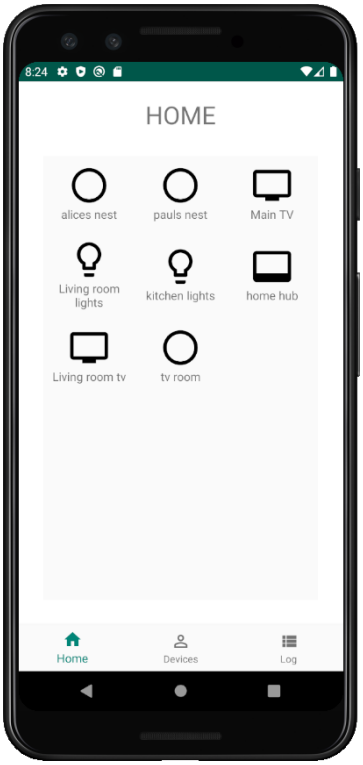

Figure 4 - Prototype application Home page

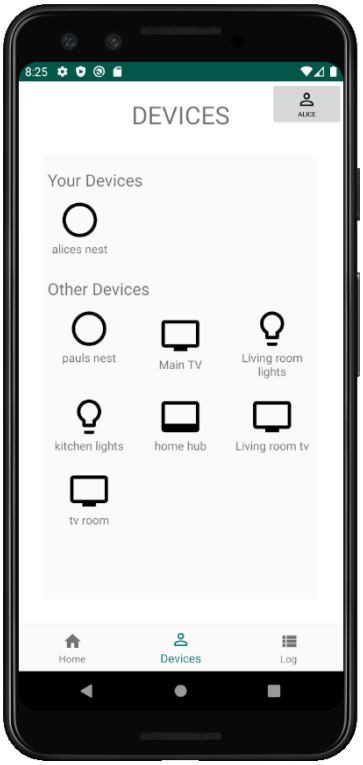

Figure 5 - Prototype application Devices page

Figure 6 - Prototype application Log page

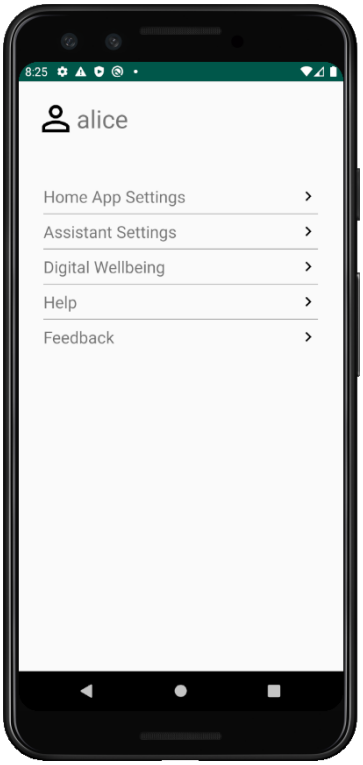

Figure 7 - Prototype application account menu page

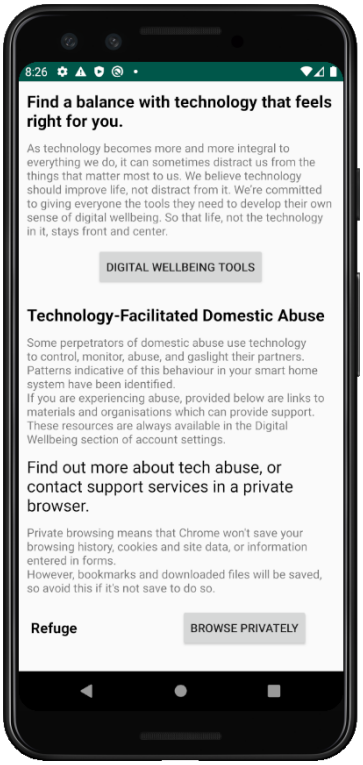

Figure 8 - Prototype application Digital Wellbeing page

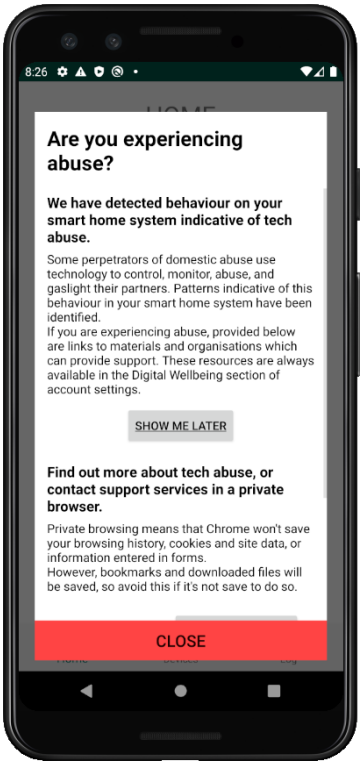

Figure 9 - Prototype application tech abuse alert

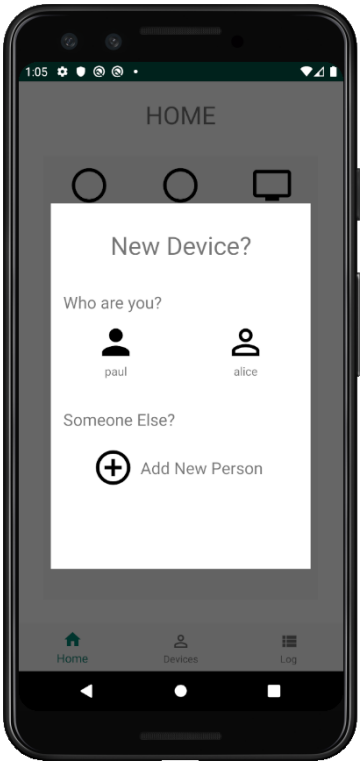

Figure 10 - Prototype application New Device pop-up