Usability Analysis of Shared Device Ecosystem Security: Informing Support for Survivors of IoT-Facilitated Tech-Abuse

Simon Parkin
s.parkin@ucl.ac.uk
Department of Computer Science
University College London
United Kingdom

Trupti Patel*
t.patel@ucl.ac.uk
Science and Technology Studies (STS)
University College London
United Kingdom

Isabel Lopez-Neira
x.lopez-neira.17@ucl.ac.uk
Science, Technology, Engineering and Public Policy (STEaPP)
University College London
United Kingdom

Leonie Tanczer
l.tanczer@ucl.ac.uk
Science, Technology, Engineering and Public Policy (STEaPP)
University College London
United Kingdom

ABSTRACT

The use of Internet of Things (IoT) devices is an emerging trend for citizens. These devices may have implications for the security of various areas of life; for survivors of technology-facilitated domestic abuse and violence (tech-abuse), a shared ecosystem of IoT devices poses new risks. Here we develop a novel adaptation of 'heuristic walkthrough' usability assessment, applying it to two readily available families of consumer smart assistant devices (Amazon Echo and Google Home). The paradigm underpinning the method considers the shared device ecosystem, and the potential threats to a person sharing smart devices with another. Prior tech abuse research informed the design of 11 tasks representing different phases of potential IoT tech-abuse. Phenomena produced by the tasks were assessed across well-defined design heuristics. Assessment was from both primary and secondary user perspectives, via a range of service interfaces (such as App, browser interface, and visual device cues). We find that many security-related elements of devices do not present usability problems, including that a secondary user has only a very limited view of the actions of a primary device user. We differentiate between features which delay or block effective use, informing potential areas for developing support solutions. For instance, findings indicate that task feedback and instructions may impact a tech-abuse survivor in an IoT ecosystem. Our results have implications for the definition of usability for concurrent users with differing expectations and needs, especially within a tech-abuse context. Our approach can inform the stakeholder conversations necessary to explore these issues across a range of other IoT devices.

CCS CONCEPTS

• **Security and privacy → Usability in security and privacy**; *Social aspects of security and privacy*; • **Human-centered computing → Walkthrough evaluations**.

KEYWORDS

home user security, usability analysis, internet of things, tech abuse, domestic violence

ACM Reference Format:
Simon Parkin, Trupti Patel, Isabel Lopez-Neira, and Leonie Tanczer. 2019. Usability Analysis of Shared Device Ecosystem Security: Informing Support for Survivors of IoT-Facilitated Tech-Abuse. In *New Security Paradigms Workshop (NSPW '19), September 23–26, 2019, San Carlos, Costa Rica.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3368860.3368861

1 INTRODUCTION

With the emergence of 'smart', Internet-connected consumer devices, individuals are increasingly able to access home appliances, entertainment devices, and online services remotely, through apps and other systems in a shared space. There have been global efforts to ensure that the technical security of these 'Internet-of-Things' (IoT) systems is sufficient, and that connected devices are safe to use (e.g., [14, 21, 35]).

The safety and security of IoT devices are of particular importance for vulnerable groups and communities. Features of digital technologies may be misused, opening up avenues for a perpetrator of domestic abuse and intimate partner violence, to monitor, coerce, or control another person [47]. We refer to this here as 'tech-abuse'. Tech-abuse can turn a cohabited space, where activities are enabled by shared devices, into one where separation and survival are paramount [46].

Mitigating tech-abuse is not straightforward, including within an ecosystem of connected IoT devices. The complexity of these systems is an obstacle not only for users, but for IoT providers and policymakers [28]. Progress must be made to ensure that survivors[1] have routes out of abuse, whether supported by institutions

*Portions of this work conducted while at Science, Technology Engineering and Public Policy (UCL STEaPP).

NSPW '19, September 23–26, 2019, San Carlos, Costa Rica

ACM ISBN 978-1-4503-7647-1/19/09…$15.00
https://doi.org/10.1145/3368860.3368861

[1]We use the terms 'survivor' and 'perpetrator', where in the literature terms such as 'victim' and 'abuser' have also been applied.

or sources of trustworthy advice [47]. Support services (such as charities and shelters) are eager to understand these new technologies [23]. There is a window of opportunity to inform guidance now, when the prevalence and deployment of IoT systems remains relatively low.

Usability analysis that includes an abuse-survivor perspective can contribute to addressing these challenges [24]. Ensuring safety from abuse in an IoT device ecosystem requires us to think differently about how usability analysis is conducted. There may be multiple smart devices, accessed by different concurrent users, through multiple interfaces (such as an App or voice command). Users may have conflicting expectations of use, making 'usability' itself difficult to define broadly. The 'security' of one user's IoT device ecosystem may be impacted by efforts by another person to 'secure' their own ecosystem, as both consist of the same devices. In cases of monitoring and control of one user by another, intervention from outside may be necessary.

The goal of this work is to inform how potential IoT-facilitated shared device threats can be identified and considered within advice, frontline services (e.g., charities and shelters), and interventions generally. This goal involves assessing all perspectives and interfaces to a connected device ecosystem in tandem. This can identify configurations and features which may produce usability inequalities between users, where these may be misused by one device user to abuse another, such as a partner (creating risks to their security and safety). Efforts to improve the situation, and reduce the capacity for misuse, can have adverse effects. This is because the 'connected' features of an IoT device which can benefit one user may benefit all users. The overarching goal requires us to scale and consolidate device analysis, to motivate and advance the capabilities of researchers and practitioners to work together. Unless stakeholders, including researchers, act to work together, analysis of future consumer devices may be fragmented, requiring further effort to scale protective efforts to the anticipated plethora of consumer IoT devices. We explore the following Research Questions:

- **RQ1:** Are there usability problems relating to IoT devices, which could impact the use and creation of advice and support in specific contexts (in this case, stages of physical control, escape, or life apart in a tech-abuse environment)?
- **RQ2:** Where usability problems exist in an IoT ecosystem, are there usability issues which may exacerbate harm, impacting not only security but also physical safety?
- **RQ3:** Where usability problems do not exist, what are the challenges for ensuring usability for concurrent users in a consumer IoT ecosystem?

We scope challenges around assessing IoT ecosystems (Section 2) and tech-abuse (Section 3). This informs our novel usability analysis approach (Section 4), and application to two families of popular IoT smart assistant devices (the Google Home and Amazon Echo). The approach specifically considers device connectedness and its implications for the security of concurrent users, and is further informed by outcomes from IoT-themed workshops with representatives of support services[2].

[2]These services generally support female survivors of abuse.

Findings are considered from multiple device *interfaces*, for the user *perspectives* of a survivor and perpetrator of tech-abuse. Results (Section 5), though not exhaustive, found that the smart assistant devices are generally usable from the perspective of different users of the same device. Feedback about changes to system configuration is lacking, with a potentially high cognitive/memory burden for any user acting to understand their IoT device configuration. In our Discussion (Section 6), we find a need to account for the shared-device threat model in future research, and to build support in environments where shared devices are equally usable for all users. We close with a review of Related Work (Section 7) and Conclusions (Section 8).

1.1 The new paradigm

Current approaches to usability analysis, such as heuristic walkthroughs [69], may be applied in a fragmented way which does not sufficiently describe a complex device ecosystem of shared use. For instance, a device may produce notifications of activity, which could impact another user's ability to preserve their privacy when using the same device.

We develop a new paradigm – shared device usability assessment for shared Internet-of-Things (IoT) consumer device security and associated threats. These devices can communicate with each other and to online services, with a capacity to monitor and control elements of the physical space that people share. The new paradigm follows principled considerations, based on an assessment of the current technology and support landscape:

- **Connected usability:** Internet-of-Things devices offer complementary interfaces to the same 'service' or 'services' (e.g., a shared online shopping account). We go beyond current usability analysis techniques (such as heuristic walkthroughs [69]) to consider multiple user *perspectives*, using a variety of device *interfaces* (inc. App, browser, linked email account, etc.), to access a service embodied by a smart device (as with home IoT systems).
- **Divergent security goals in a shared space:** We employ the approach of *sequential* usability analysis (one user following another). This approach allows us to model concurrent users with differing (security) goals, and to explore potential (harmful) implications of IoT systems (Section 3.1). We frame divergent goals and tasks by defining the security-related mechanisms [72] and phenomena (Section 2.3).
- **Negative implications of 'connected' usability:** Usability improvements can have negative implications for an individual, if those improvements make it easier for another person to control shared devices. We re-think how the outputs of a usability analysis are applied (relating outcomes to different support stakeholders). Violations of usability heuristics [54] may indicate where support can – or should not – be targeted, to minimise the risk of harmful side-effects in the cyber-physical space.

2 BACKGROUND

In this section we describe our overarching considerations and approach, before focusing on the application to tech-abuse in Section 3.

2.1 Supporting secure use of consumer IoT devices

Efforts to ensure that IoT devices are technically secure are active, pursued by various governments and manufacturers, e.g., the Internet Society [35] and the UK Government [14, 74], and more broadly by e.g., ENISA in the EU [21].

Consumer IoT ecosystems may consist of multiple devices, such as smart assistants and smart home appliances. An individual may use a range of devices to access the same service or account. Within consumer IoT, security-related features (such as permitted user accounts, and activity histories) may be accessed through various interfaces, rather than just one interface in isolation. Different individual interfaces may be used based on context, such as being in the same room as an IoT device, or near to the home. Vaniea et al. [82], for instance, consider the view of the human, the phone (with App) and an IoT device during setup. The diversity of IoT device interfaces contributes to the complexity of providing support.

We must then acknowledge that there is a multi-device, multi-interface, and multi-user ecosystem around a series of service accounts, as broadly illustrated in Figure 1.

Producing clear and actionable security advice which scales to cover many IoT devices and contexts of use is challenging. This points to a need for defenders to share expertise and keep pace with the advancements of consumer IoT devices.

For IoT systems, as for IT technologies generally, devices ought to uphold conditions that allow individuals to use the devices without 'overstrain' or a need to be aware of the latest technological trends [49]. Indeed, it should be acknowledged that "everyday people manage everyday Things" [40]. It is useful here to differentiate between different members within a smart home, where technology may be managed by one or another member of a shared living space. Zeng et al. [86] distinguish between users who manage a smart device, and 'incidental users', who may have limited access to the features of the smart home environment. The latter may have reduced awareness of security issues.

At present, many smart home devices are controlled via a smartphone app, paired with each device [31]. A user may authenticate to a device's app using a password. Smart assistant devices such as those in our study may be activated by a 'wake word' [68], to record, process, and enact a spoken command. Where users share a device with the capability to record a query, any user may initiate recording [17]. The user whose account is linked to the device can specify only limited restrictions for other users. There may also be third-party apps and integrations (e.g., IFTTT) [87], which implement rules to combine actions or integrate with other cloud/online services.

2.2 Potential harms in a connected device ecosystem

The challenge of mitigating technology-facilitated harms is already recognised in industry standards and in the research community. Referring to ISO 25010 [36], the need to ensure technology is technically secure is complemented with the need to ensure secure and safe usage. ISO 25010 refers to 'Freedom from Risk', including "Health and safety risk mitigation".

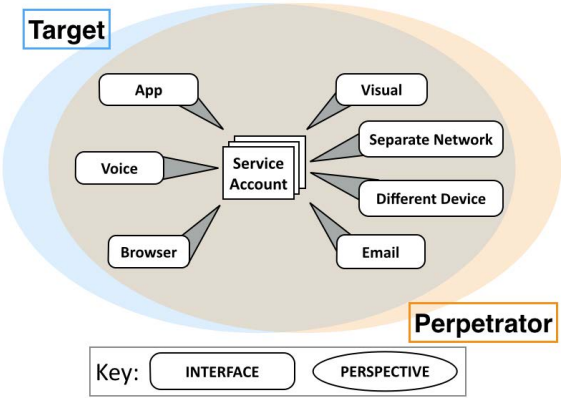

Figure 1: Perspectives and Interfaces onto a service account in a shared, connected device ecosystem.

This aligns with the need for a 'fair' IoT [43], including that a person will not suffer as a result of circumstances outside of their control. It also aligns with foundational principles of usable security. A need was identified by Zurko in 2005 [88] to *"give all users [...] security controls that protect them, [and] their systems, [...] that they can use appropriately in the dynamic, pervasive computing environments of the present and the future"*. In the current analysis, we are reconnecting the need for both security and protection. We broadly propose a direction of usability analysis toward freedom from risk in an IoT device ecosystem beyond but including technical threats.

Usability analysis arguably assumes that the 'evaluator' is an expert who knows the device under examination. While the security standards for IoT devices remain fragmented [7], the challenge of scaling analysis is compounded. We, thus, require a means to assess combinations of smart devices, but may also need to re-assess individual devices and combinations over time as they are updated. This would be the case if it cannot be assumed that devices adhere to any particular standard of functionality or behaviour.

2.3 Studying mechanisms of shared devices

In the interests of contributing to general knowledge for security researchers in the area (and specifically in tech-abuse, as in Section 3), we examine *mechanisms* [72] of IoT systems and related user-facing threats for the devices being studied here. Mechanisms consist of entities (parts) and their interactions in activities (what the "bits and pieces do" [34]), organised so as to be responsible for the phenomenon of interest. Software and technologies change over time, as can be the case for IoT devices and other *engineered* mechanisms [29].

The phenomena we test for are violations of usability heuristics, rather than specific technical outputs coupled to a specific device function. Nielsen [53] defines 'major' usability problems as having the potential to confuse users or induce errors (where here we include 'blockers' to task completion within this), and 'minor' usability problems as producing inconvenience or delays (which can be critical when evading abuse [75]). We use violations to frame

our findings, as being sufficient to identify areas for further, focused intervention.

Certainty about what occurs or does not occur as a result of using a function has added importance. We then also discuss phenomena that is not observed (i.e., usability heuristics not being violated); This informs the view of the capabilities which concurrent users may have to influence each other's use of IoT devices.

The assessment of usability with multiple devices has been applied elsewhere, such as to study device pairing [79]. In collaborative work, Pinelle et al. [60] proposed to study not only individual actions, but also collaborative actions, focusing on tasks at a 'mechanical level' (representing *"things that will be common to a shared task even with a variety of social and organizational factors"*). Where Pinelle et al. consider multiple users working toward a shared goal, this is analogous to harmonious use of IoT devices in a shared environment. To inform the security analysis, we require a method to explore shared use of mechanisms for differing goals, and hence model users acting to perform individual tasks in a shared interface without interference from other users.

2.4 Experimental procedure

It may not be possible or appropriate to explore the usability of IoT devices directly within a climate of harm, particularly in an abusive context. Instead, we conducted a lab-based analysis adapting the *heuristic walkthrough* framework [69], which in the original form combines heuristic evaluation [55] and cognitive walkthrough [83] techniques.

The heuristic walkthrough approach combines free-form evaluation and usability heuristics from the former, with user task questions to highlight important interactions from the latter. A similar approach has been applied to examine, for example, configuration issues in the Firefox web browser and Outlook email client [25].

The original heuristic walkthrough approach requires a set of user tasks (Section 4.3), applying usability heuristics and 'Thought Focusing' Questions (TFQs). A *first pass* is guided by the prioritised task list and TFQs. Usability heuristics then guide a *second pass*, exploring system aspects and potential usability issues more broadly. The outcomes of the task analysis were recorded and stored securely and accessible only to the authors.

The TFQs, adapted from Seers [69], are as follows:

(1) Will a user know what they need to do next?
(2) Will a user notice that there is a control available allowing them to accomplish the next part of their task?
(3) Once a user finds the control, will they know how to use it?
(4) If a user performs the correct action, will they see progress being made toward completing the task, and appropriate system feedback?

Research of sequential security-related tasks suggests that one task can impact completion of subsequent tasks [12]. Similarly, some actions may escalate other forms of abuse [24]. We model the dynamic of concurrent users of a connected device ecosystem – and the intrinsic connectedness of IoT consumer devices – by maintaining two perspectives through both phases of the usability analysis. We refer to these as the primary and secondary users, to determine the ability of the latter to observe (impact privacy) or alter configuration choices of the former (which may be used by either a perpetrator or survivor). Further to this, the survivor and others in the household are assumed to have equal access to App and browser interfaces (that the primary user and controller of devices are not necessarily the same [24]). The following are then TFQs representing the secondary perspective:

(1) Once a control is used, does this impact a secondary user's ability to use or alter the same control?
(2) If a primary user performs the correct action, can other, secondary, users see that progress is being made toward completing the task?

We regard incidental sight of activity with the same caution as deliberate monitoring. The presence of either behaviour in a shared environment may bring with it the possibility of harm if noticed by an attacker (including a perpetrator of tech-abuse, Section 3); activity may be noticed by a survivor, informing plans to escape. We do not tie either the primary or secondary user perspectives (Section 2) to a survivor or perpetrator, as the consequences differ between these cases (with implications explored in Sections 5 and 6).

The second pass is informed by the usability heuristics defined by Nielsen, as summarised in [54] and reproduced below:

- **Simple and natural dialogue:** Dialogues should not contain irrelevant information; information should appear in a logical order;
- **Speak the user's language:** Use words, phrases and concepts familiar to the user, rather than system-oriented terms;
- **Minimise the user's cognitive load:** There should be no need to remember information from one dialogue to another;
- **Consistency (in meaning):** Users should not need to wonder if different words, situations, or actions are the same.
- **Feedback:** Always keep users informed about what is going on, in reasonable time;
- **Clearly marked exits (from unwanted states):** A clearly marked "emergency exit" that avoids an extended dialogue;
- **Shortcuts (to speed up interaction):** 'Accelerators' which may speed up interaction for more experienced users who know about them;
- **Good error messages:** Expressed in plain language (no codes), and constructively suggest a solution;
- **Prevent errors:** A careful design which prevents problems from occurring in the first place;
- **Help and documentation:** Any necessary documentation ought to be easy to navigate, focused on the user's task, and provide concrete steps.

Evaluators would normally assign severity ratings, to identify problems to solve first. Here, the intention is to document problems, and consider them post-hoc for a range of stakeholders. Many different parties are involved in consumer IoT security (e.g., policymakers, manufacturers) and reducing harms to survivors (see Section 5.4 and Section 6). Our paradigm informs support interventions, by assessing not only inherent usability problems, but also the potential harms of already usable features, and the potentially negative, unintended implications of plans to resolve usability problems).

3 CASE STUDY – IOT-FACILITATED TECH-ABUSE

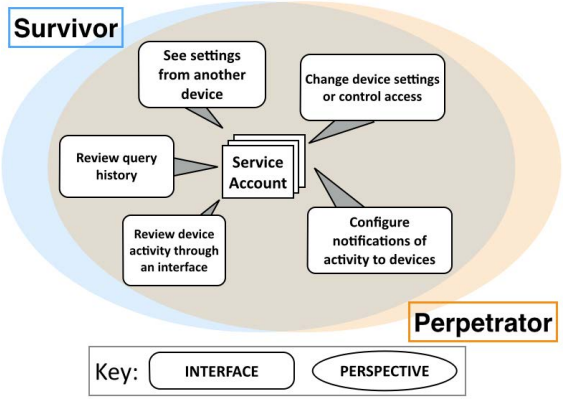

Figure 2: Potential Perspectives and Interfaces onto a service account in a climate of tech-abuse (with potential examples).

To consider the scale of intimate partner abuse, reports of (US) Centers for Disease Control and Prevention data indicate that nearly 27 million women and 16 million men in the United States have experienced severe physical violence by an intimate partner [47]. In the UK, 1.3 million women and 695,000 men have experienced domestic abuse[3]. There is evidence that the majority of those who have suffered intimate partner violence (IPA) are female, with some national-level reports of up to 70% of women having experienced IPA[4]. Regarding tech-abuse, for 85% of Women's Aid (UK) research respondents, the abuse they received online from a partner or ex-partner was part of a pattern of abuse they also experienced offline[5].

It is recommended [75] that developers should test solutions to tech-abuse problems in a range of contexts, including with LGBT+ and BAME communities, to ensure suitability and relevance. It has also been documented recently that migrant women are particularly vulnerable to tech-abuse [16].

3.1 Threats in an IoT ecosystem

'Things' in the Internet-of-Things (such as smart assistants, smart locks, and other connected devices) can have multiple owners [40]. These devices will have legitimate features which could potentially be used to monitor or control another person in a shared environment [27]. The following potential threats (reproduced from [27]) – from other users of the same devices – are informed by research of existing forms of tech-abuse (such as via social media).

- **Wearable devices:** Could allow perpetrators to track and monitor movements.
- **Phones:** Could provide the perpetrator with an access point to control various IoT devices.
- **Laptops and tablets:** If accounts between devices are linked, a perpetrator could change or monitor device settings.
- **Remote control of heating, lighting and blinds:** May be switched on or off from afar.
- **Audio recording:** Could enable remote monitoring.
- **Voice control:** A perpetrator could contact a person, or trace and review their history of commands and purchases.
- **Router:** Connects all smart home devices to the Internet.
- **Security cameras and TVs:** Could facilitate remote monitoring and online stalking.
- **Smart security:** Could provide (remote) access to doors.

Attacks in this context may not be sophisticated, using existing features intended for end-users in unintended ways, to cause harm and distress (with examples illustrated in Figure 2). Freed et al. [24] point to 'simple' attacks such as being the *owner* of an account, as well as being able to guess a person's account password. We focus on *attacks through standard features* used to *monitor and/or control* another person. There are already examples of perpetrators of tech-abuse tracking others through roadside assistance systems [63] or phone-finding apps [80], or controlling the smart home from afar through Internet-connected thermostats and door locks [6].

Communities and governments are acting to limit existing forms of tech-abuse through e.g., social media or smartphones [33], where further empirical evidence would be of benefit. With the proliferation of IoT devices, coordinated efforts to understand and mitigate tech-abuse similarly need to operate at scale.

The picture of all of the relevant stakeholders is complex. Support for those affected by tech-abuse can be taken over by voluntary and statutory support services. This can also involve law enforcement when there are incidents; policy-level oversight to inform efforts at scale; manufacturers and developers to consider changes to the devices themselves, and; support for the consumer/end-user themselves within their specific context of use. Guidance and support is one avenue to develop mitigation strategies, while usability improvements are also critical for users with less technical knowledge of smart devices [86].

It may not be conducive to simply remove devices from the shared environment as they often serve positive purposes (such as legitimate use of the smart home). They then require an approach of positive security [66] which would normally protect positive uses of digital technologies [11].

Protective advice (and usability improvements) can potentially have unintended 'side effects' (as noted in prior research on tech-abuse [23]). Interacting with a device may change how it operates for others, similarly impacting a survivor's circumstances.

3.2 Managing security and privacy in an abusive environment

There is a need to ensure that survivors can access the support that is intended for them [81], and be able to do so quickly [75]. Guidance and support also ought to be useful for survivors, with no way for it to be misused by perpetrators [2].

The management of devices has been considered as part of relationship dissolution [67] and the breakdown of a cohabiting relationship [48]. If tech-abuse is happening, a survivor may have

[3]https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/domesticabuseinenglandandwales/yearendingmarch2018
[4]http://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures
[5]https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/

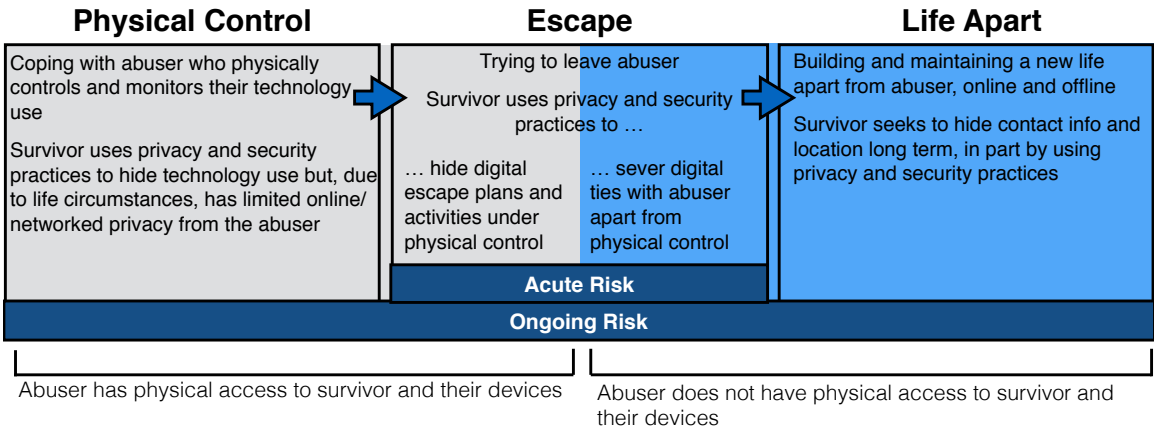

Figure 3: Phases of technology-facilitated abuse, adapted from [47].

limited or *reduced* access to device features or the device itself, or find their access controlled or monitored by a perpetrator.

Where research often points to the lack of usability of security- and privacy-related device features, there is a further need to consider whether features can be used skillfully under *increased stress and risk* [47] (for instance when trying to use a device and at the same time evade detection by a perpetrator). The capabilities of an individual then need to be considered when preparing support [56], in terms of how technologies extend to meet the user needs, and match the needs and uses they have for their devices. It may also be necessary to ensure that positive uses are not restricted (such as being able to communicate with family and friends).

The capacity to escape from abuse may be limited further by reduced access to – and accessibility of – instructions on how to use security and privacy mechanisms [47]. When survivors of abuse proactively search for information about the use of technologies, there may be barriers to finding it [23]. We are then interested in how IoT devices inform and support a user (at any level of expertise), and so we must also assess *adherence to design principles* when evaluating devices and the surrounding technology ecosystem.

3.3 Phases of abuse

Kotz and Peters describe the IoT device lifecycle [40]. We combine this with the stages of tech-abuse defined by Matthews et al. [47] (see Figure 3) to frame related challenges in an IoT device ecosystem.

3.3.1 Device configuration. Devices must be configured securely [40]. We make no assumptions about who manages device configuration, but there are implications if it is the perpetrator, as discussed in Section 3.1. Technology-related responsibilities, such as managing an online account, may also be shared [48] (or access shared, perhaps under coercion).

In a trusting environment, just as in an abusive one, a person may be privy to passwords used to secure an online account [23], though this also means that users may have equivalent access to an account or device. A party in the relationship may be at risk of harm if users no longer share a 'threat model' [86], be it because of disagreement, or abusive behaviour. An individual's capacity to otherwise weigh up personal security and privacy decisions [52] may be reduced, or at worst removed entirely by a perpetrator.

3.3.2 Physical control. A device may have multiple owners [40]. Here, the definition of a 'secure' configuration could potentially be skewed to favour the perpetrator (either directly or through coercion of the survivor). A configuration that is 'secure' for the perpetrator may not be secure for the survivor. This prevents them from working around the technology or using it as they would want to. This then leads to needing to use devices in a way that cannot be observed or where records can be removed afterwards, or to use devices which are not known or observable, or have reasonable reasons for using a device in a particular way [47].

3.3.3 Escape. IoT devices can be used to control other devices in the home. Therefore, any actions to hide technology use will already require the hiding of digital escape activities under physical control. The capacity to escape abuse may be reduced, according to the level of interconnectedness in the shared smart environment; a reduction in access to digital communications can reduce access to help, social relations, and work [47]. There is then a need to consider whether 'escape' would be satisfactorily effected by simply leaving the smart home, or whether it is necessary for an actor in this environment to 'disentangle' online accounts, so that the online status "[matches] the offline one" [48] after leaving abuse.

3.3.4 Life apart. The process of reaching a life apart can potentially take weeks or years [58]. The pervasiveness of IoT connections to online accounts must then be considered, as part of the 'moving on' sub-phase noted by Matthews et al. [47]. Someone who previously used a smart device may move away or discard a device, where these intentions come with their own risks for the device user [40].

4 METHODOLOGY

Here we describe an application of the shared device' usability analysis approach (Section 2.4) to explore security-related challenges in IoT-facilitated tech-abuse (as described in Sections 3.2 and 3.3).

4.1 Scoping via support service engagement

Secondary analysis was conducted of the outcomes of two workshops, each attended by 40-50 representatives of support services and other related organisations supporting victims of tech abuse and domestic abuse / violence [45]. The workshops were arranged with a group of support services known to the 'Gender and IoT' project research team[6]. The first workshop aimed to assess the concerns and research needs of organisations working with victims/survivors, particularly those affected by tech-abuse (arranged around group discussions of the impacts and potential risks of consumer IoT devices). The second workshop built on the outcomes of the first, with group discussions around the guidance that support services need, based on preliminary (desk-based) analysis of the capabilities of IoT devices.

Workshops involved attendees (support representatives and academics alike) discussing IoT devices and related issues in small groups on separate tables (where known limitations of focus groups apply [1]). An anonymised transcript of the discussion on each table was produced, where each workshop produced multiple transcripts. The workshops had IRB approval at UCL.

Thematic analysis [8] was applied to transcripts to identify themes. Two of the authors independently coded the group transcripts, discussing a codebook at intervals in the process. Themes emerging from coding were narrowed to those with implications for use and advice for IoT consumer devices, as follows:

- Solutions involve a range of *stakeholders*, requiring a joined-up approach that brings together support services, police forces, law and government, technologists, and the developers of technology devices;
- Advice and support may be needed across *different contexts* within a survivor's life (not just home life), across different channels and potentially a long time;
- Victims may perceive being monitored, but not how – or with the evidence that – it is happening;
- IoT-related threats were not seen to be prevalent, but were a concern (though this may have been as a consequence of the workshop themes);
- Advice to victims generally focused on resetting or disposing of devices, and technology was also seen as an enabler of abusive behaviours that developed unwittingly;
- Modifying a device may in some cases not be possible (for instance in a coercive relationship);
- The pace of change in technology may change the implications of specific advice; Support services conveyed that they were lacking in awareness and skills;
- Technology with legitimate uses may be appropriated and used to control or monitor;
- A key concern was that advice may exacerbate an abusive situation, if the related risks in applying the advice were not considered.

These themes align with findings from existing research of tech-abuse (e.g., [24, 47]). We further identify that IoT-facilitated tech-abuse is an emergent concern for support services.

The analysis approach described in Sections 2 and 3 is then required to inform the last two findings, to determine how legitimate features could be used control and monitor another person. The approach is also useful for determining where advice, and support more broadly, can be targeted so as not to disadvantage a survivor.

4.2 Devices and interfaces

We selected popular devices which are available both online and in-person at stores. We then chose to study devices produced by Amazon and Google – as of 2019, it is estimated that Amazon and Google account for 91.9% of smart/voice assistant IoT device models [42]. The devices are the Google Home (MFG 03/2017) and Amazon Echo (2nd generation) smart assistant devices. For testing purposes, the Home and Echo are regarded as equivalent to their smaller counterparts, the Google Home Mini (MFG 02/2018) and Amazon Echo Dot (2nd generation) respectively.

Tests were conducted using the Google Home and Amazon Alexa smart assistant apps, both running on an iPhone 6 (app versions 2.9.118 and 2.2.250839.0 respectively) and a Motorola Nexus 6 (Android) (app versions 2.8.15.6 and 2.2.250163.0 respectively). Use of two handsets/apps was crucial for modelling concurrent users (see Section 2.4). Browser views were monitored by researchers on separate computers alongside the phones and IoT devices.

For each test listed in Section 4.3, we explore a range of what we refer to here as *interfaces* (where applicable to the test) – see Figure 1, Section 2. These are: App view (including a secondary user); Browser view (service account); Browser view (linked email account); Voice retrieval; Visual/physical interface, and; Authorised device on a separate network.

4.3 Tasks under analysis

We assume a "UI-bound" perpetrator [24], and assume users enact only well-known functionality offered by an IoT device's interface(s) to perform specific tasks (Section 4.3). When configuring each smart assistant device, the researchers accepted all default settings, in effect analysing a "default-bound" IoT system. We note here that our results represent a point in time, and were time-constrained to only having the devices powered on and in use during and around analysis (to support internal validity [41]).

Tasks represent observed phenomena; that is, a phenomenon of or relating to tech-abuse, and a suggestive mechanism by which it might occur. These are tasks which may be enacted by a well-meaning user who is not in a climate of abuse, but which may be appropriated by either/both a survivor or perpetrator of tech-abuse.

As an example, a perpetrator might seek a way to find out how a smart assistant device has been used by others in the shared environment (as in task TB.1 below); a perpetrator, or a survivor, might aim to render a smart assistant device inactive without it being visible to another person through some or all of the *interfaces* (Section 4.2). These tasks represent possible overarching goals, rather

[6] http://www.ucl.ac.uk/steapp/research/projects/digital-policy-lab/dpl-projects/gender-and-iot

than being an exhaustive set of tasks. Tasks are mapped to abuse *phases* (as in Section 3), though any or all tasks may be enacted in each phase.

A. Configuration: Any user of technology in the shared environment. Tech-abuse may nor may not already be occurring/recognised at this point. This also addresses the capacity of a secondary user to see or alter actions in subsequent stages.

- **TA.1: Perform initial setup.** A user may be prompted to conduct a setup process through one or any of the various interfaces described in Section 4.2.
- **TA.2: Configure an account hierarchy.** This depends in part on whether other users then do not have an equivalent level of control.

B. Physical control: A survivor may act to hide activity. A perpetrator may act to develop a complete view of activity across the connected device ecosystem.

- **TB.1: Review historical queries and actions.** It may be that query and activity information is accessible to those who made the changes, and also other users of the same device(s).
- **TB.2: Complete another user's action.** This includes 'activating' capabilities of another linked user or their devices.
- **TB.3: Configure notifications to different devices.** Notifications to devices/interfaces may be configurable to varying levels of granularity.
- **TB.4: Disrupt always-connected device activity.** A dormant interface may appear equivalent to an inactive one.

C. Escape: A survivor may reduce the visibility of their actions.

- **TC.1: Remove records of activity.** This can include deletion of information provided to the devices, but also changes to recorded details.
- **TC.2: Visible configuration of devices.** This includes those set by other users, but also whether an individual user is able to 'recall' settings that they have made themselves.
- **TC.3: Break down a link to an IoT device.** It may be possible – or not – for a user to undo the connection between an IoT device and other interfaces.

D. Life apart: A survivor would ideally be able to move on, and be able to build new connections with technology apart from the perpetrator. A perpetrator may act to reach the survivor or return them to Physical Control.

- **TD.1: Obtain a manifest of account connections.** It may not be necessary for a user to keep a running memory of the accounts that they have connected and shared with other users of the same IoT devices.
- **TD.2: Replace a connection with an IoT device.** Undoing a connection to an IoT device is not the same as replacing that connection with another IoT device.

4.4 Limitations

The analysis is from the perspective of researchers, rather than an actual user of the device or a situation of tech-abuse. To account for this, the analysis protocol was informed by workshops with support service representatives on emerging issues around consumer technologies.

Across the workshops and device analysis, we observed that prior guidance on the capabilities of IoT devices can potentially be outdated. We have not accounted for the effects of time and technology change. This raises the possibility of results being inconclusive (rather than the tests themselves) due to changes in the devices under study. In designing the analysis to consider the dynamics between multiple device users, one intention is for researchers in the future to apply the analysis protocol described here to reevaluate whether advice still holds when device functionality changes.

5 RESULTS

We are mindful of the potential 'misuse' of protective research by attackers [15], where this is a concern in tech-abuse research [2]. Following an approach defined by the Medical Research Council (MRC), Biotechnology and Biological Sciences Research Council (BBSRC), and Wellcome Trust [51], we take steps to limit providing information *"that could be directly misapplied to pose a significant threat with broad potential consequences to public health and safety"*.

We act to *"limit dissemination, e.g. by publishing only part of the research results"* [22]; We provide overview results, without identifying specific entities or activities which make actions possible.

We do not report on specific 'tasks' or 'interfaces'. We also do not report the specific phenomena we observed, but instead report observed usability problems and design principle violations as the unit of measurement for the case study, as a proxy phenomena (in Sections 5.1 and 5.2, and Section 5.3 respectively).

Though communicating results in security is not trivial [73], we believe this approach is sufficient to encourage focused collaboration between stakeholders. One stakeholder acting in isolation to fix a user interface problem is arguably limited in their potential to address IoT-related harms at scale.

5.1 Capabilities of primary perspective

Referring to the Thought-Focusing Questions (Section 2.4), the issue of a user "knowing what to do next" effectively becomes a question of "knowing what can be done next". For instance, many features of each device, and the service accounts they are linked to, can be accessed through a subset of the *interfaces* to the device. However, we found that there is reliance on the user knowing which features are available in advance, especially through perspectives which do not readily communicate a list of available features to even a motivated user. This would impact efforts to elude 'Physical Control' (3.3.2) or to effect 'Escape' (3.3.3), if a survivor were a 'secondary' user to a primary user who was a 'tech-savvy' perpetrator.

Once feature controls were located (through, for instance, App menus, or by accessing a service through the browser), they seem generally intuitive for both of the smart assistant devices. The Alexa and Home apps are functionally the same on the separate phone handsets (running iOS and Android), indicating no advantage in using different kinds of handsets. The assessed IoT devices behaved

in similar ways for the majority of tasks. Both devices proactively provide direct links to (limited) help and guidance. The two devices then share some common functionality, implying that expertise in using one device is in part transferable to another (as also suggested by the similarity of results in Table 1). This may equalise expertise, but either a survivor or a perpetrator could be empowered with knowledge from elsewhere.

Supporting advice on how to use device features is variously available to a user through the different interfaces, but security and privacy are seemingly not included in what is immediately provided; there is a need for a user to proactively search for it. This makes 'Configuration' (3.3.1) a critical stage, especially if there is one user setting up and managing devices and others not involved in this *phase*. Other research has found that, for instance, mobile technologies may be used to 'isolate' a victim [85]. A user (primary or secondary) might only act to have some influence over the 'Configuration' if they are already anxious about controlling digital privacy [19] or proactively interested in the first instance [26]. Conversely, Williams et al. [84] point to a disparity in the secure use of consumer IoT devices, that devices will be purchased but protective action not taken.

Tasks representing the 'Escape' phase had the greatest capacity to delay a primary or secondary user (see Section 5.3), with the potential for confusing context-switches between various interfaces. This may impact a survivor seeking to navigate away from the device ecosystem, but also delay a perpetrator if they are switching between contexts or are limited to using a subset, in effect hampering their efforts to monitor or control [24]. Features to decouple accounts ('Life Apart', 3.3.4) exhibited some differences, implying that device-specific advice is critical in this phase.

5.2 Capabilities of secondary perspective

Following the 'Physical Control' tasks (Section 4.3), we did not see phenomena that indicated that a secondary user could use any of the perspectives to observe a linked device (such as another user's smartphone or computer). Visibility of the status of the smart assistant devices from outside a host network was limited. There were, however, a few instances of a secondary user, within the same network, having the opportunity to incidentally observe indirect indicators of a task being performed by a primary user. This could be of concern if a survivor is assuming that their activity as a primary user is not being observed.

When considering device use across the different interfaces (Section 4.2), some interfaces provide information and options relating to device functionality which is not available through other interfaces. This includes specific features of the smart device, but in some cases also the information that relates to a feature (including what it is and that it exists). Combined with the potential cognitive burden of switching between interfaces, this could complicate any efforts to support a primary user to elude 'Physical Control' or to effect 'Escape'.

Changes to settings are not immediately obvious, and must be found or noticed by a secondary user. Device actions were basic, with few interim steps. As such, it was not possible for a secondary user to see interim progress being made toward successful completion of a task. The act of looking at any of the settings or content is not logged and cannot be retrospectively checked. This does, however, support novice users who wish to explore features available to them without other users knowing (though this could be leveraged by either a perpetrator or survivor).

Direct notifications do happen in some cases, for instance to support a primary user who has left the device ecosystem ('Life Apart'). This phase was where we found inconsistencies between the devices, in terms of what was possible and through which perspective to enact escape and ensure having left the ecosystem. In the area of domestic abuse/violence, there is clear benefit in developing technologies which empower survivors [10] and which help to rebuild trust in technology; consistent ways to inform disconnected users could then be useful for finding a 'new normal' [46].

Table 1: Overview outcomes for concurrent-user usability analysis across the four phases of abuse. Each 'dynamic' indicates whether a secondary user/perspective may experience a particular kind of usability violation (delay or obstacle) when observing or acting upon the activity of a primary user/perspective (who may also be experiencing usability problems). An example would be a solid square for *'Pri: N'* (row) and *'Sec: N.'* (column), indicating no observed usability violations for a secondary user using the interfaces after a primary user. We obfuscate which device is being referred to (devices analysed separately, indicated by the bold dividing line).

1^{st} Dev.	Config.	Phys. Cont.	Escape	Life Apart
Sec.:	N. Mi. Ma.	N. Mi. Ma.	N. Mi. Ma.	N. Mi. Ma.
Pri.: N.	■ □ ■	■ □ ■	■ ■ ■	■ □ □
Pri.: Mi.	□ ■ □	□ □ □	■ ■ □	□ □ □
Pri.: Ma.	□ □ □	□ □ ■	□ □ ■	■ □ □
2^{nd} Dev.	Config.	Phys. Cont.	Escape	Life Apart
Sec.:	N. Mi. Ma.	N. Mi. Ma.	N. Mi. Ma.	N. Mi. Ma.
Pri.: N.	■ □ ■	■ □ ■	■ ■ ■	■ □ □
Pri.: Mi.	□ ■ □	□ □ □	■ ■ □	□ □ □
Pri.: Ma.	□ □ □	□ □ ■	□ □ ■	■ □ □

KEY:
□ = No observed usability violation(s) 'dynamic' observed in our analysis for a specific phase.
■ = Usability violation(s) 'dynamic' observed for the secondary perspective, using interfaces after the primary perspective.

5.3 Usability violations across heuristics

Table 1 provides a high-level overview of observed usability heuristic violations (as used during the evaluation 'second pass', as in Section 2.4). Each phase includes tasks with minor or major usability violations, implying that advice to survivors may need to address specific devices or features. All phases included major violations for a secondary user trying to override or reproduce a primary user's

Table 2: Outcomes for evaluation of the smart assistant devices in sum, across the different phases of abuse. This includes usability heuristics and heuristic violations, which may be minor (inconvenience or delays) or major (confuse users or induce errors).

Usability Heuristic	Config.	Ph. Cont.	Escape	Life Ap.
Simple dialogue	□	□	♦	□
User's language	♦	□	□	♦
Minimise load	♦	■	■	□
Consistency	■	■	■	■
Feedback	□	♦ ■	♦ ■	■
Marked exits	□	□	□	□
Shortcuts	■	□	□	□
Good errors	□	□	□	□
Prevent errors	□	□	□	□
Help/documents	♦ ■	♦	♦ ■	♦

KEY:
□ = No observed usability violation(s).
♦ = Minor usability violation(s) observed.
■ = Major usability violation(s) observed.

actions, as another person should not normally be able to interfere in a primary user's actions.

The combination of no observed usability violations for a primary user, followed by Major violations for a secondary user (top-right corner for each phase, in Table 1), indicates that for some tasks a secondary user cannot see or impact what another user has done. Major violations for both users imply simply that the device is not capable of enacting a task. The Escape phase has many dynamics of primary/secondary user/usability barriers, and so advice would have to targeted, concrete and correct. 'Life Apart' points to 'major' usability violations, in the sense that a primary user would no longer be part of the device ecosystem once they have disconnected from it.

All *phases* included one or more tasks which demonstrated non-violations of usability heuristics (a solid box in the top-left of every phase, as in Table 1); there were many features which appeared usable (no observed usability violations). This benefits all concurrent users equally.

Table 2 summarises heuristic-specific violations. Again, the two smart assistant devices behaved similarly, so we evaluate the devices as a class of device rather than individually. Each box represents whether non-violations or minor/major violations occurred for any of the design heuristics (Section 2.4) across the different interfaces listed in Section 4.2. As the devices were functionally similar, Table 2 summarises issues found across both devices. A row with more solid boxes implies a fundamental challenge in using the device(s); a column with more solid boxes in it implies that providing actionable support could be more complicated.

5.3.1 Dialogue and language. 'User's language' and 'simple dialogue' were generally clear. Mobile and Internet skills can translate into good IoT skills [13]. This suggests that guidance on how to use (potentially unfamiliar) IoT devices can leverage experience with more familiar concepts such as mobile and Internet use.

5.3.2 Consistency. 'Consistency' was a persistent issue across phases. Some features relating to the same device were presented differently depending on which interface was in use. This also points to major blockers, as there was generally no one interface which contained all of the available information and features found across all interfaces.

5.3.3 Feedback. 'Feedback' was limited throughout the tasks representing 'Physical Control', 'Escape', and 'Life Apart'. Tasks representing 'Escape' had the most minor violations between perspectives, where ascertaining system state and current device configurations can require a review of several interfaces.

Both devices were similar in usability, with a few subtle differences. Generally, a secondary user was not able to determine much of the activity of the primary user. This is advantageous for a survivor, as a primary user, trying to hide their activity ('Configuration', and 'Physical Control'), but problematic for a survivor who wants to ascertain the device configuration, to then determine how to act outside of it ('Escape'). 'Feedback' was a blocker for a secondary user – generally, they could not see what the primary user had done, and would not be notified directly of changes made by the primary user.

Notifications are for the most part not sent – to either primary or secondary user – to confirm that a control has been used successfully. When considering the UI-bound nature of the tasks, there is no 'history' or log of features having being used over time (though this is generally the case with home user devices). A critical result relates to the lack of phenomena to indicate that progress has been made in successfully using a feature; there is a general lack of direct notifications to users when device state has changed. This impacts both primary and secondary user perspectives.

5.3.4 Marked exits and Shortcuts. 'Shortcuts' for users are hinted at with more advanced features that hook in to the functionality of other devices in the home IoT ecosystem. These rely on the user being proactive, to invest in figuring out how to make the features work. This would normally be a minor usability problem, in that these 'accelerators' (Section 2.4) are indeed unseen to novice users. However, they could remain so, keeping a user in a novice state until they personally act otherwise. Attempts to learn how to use features may also take time and be visible to others. These issues would be a blocker during 'Configuration', but perhaps not for subsequent phases (where a survivor may forgo discovering features, and instead work around them and the device).

5.3.5 Good errors. 'Error messages' are clear, where this hints at the relatively restrictive nature of how the smart devices can be used (though this serves at the same time to 'prevent errors'). We found no evidence of errors during testing, but the converse was the case – as found elsewhere [37], configuration was restricted and simplified. This is in line with other IoT devices where device complexity is hidden, as with e.g., digital switches [82].

Actionable advice could become irrelevant over time if device features change, and general advice may require the reader to translate it to their own context [23]. One stumbling block experienced early-on in the analysis is that online, up-to-date guidance sits alongside

out-of-date guidance, most notably online (noted elsewhere as a potential factor in negative security-related experiences [64]). It is not always obvious that tips and tricks do not apply to the current version of the software or the device, which is key if *one device or any one of its interfaces can change functionality across its lifetime*, as we found during this study. When troubleshooting, it is arguably then not enough to identify the device, but also app versions, which interfaces a survivor has access to for a support service to give guidance about (as in Section 4.2), etc. This points to the need to involve a wide range of stakeholders to differentiate and signpost 'good advice' to prevent errors based on incorrect information.

5.3.6 Prevent errors. Decoupling devices from interfaces (other non-smart devices) can be potentially confusing, as features interchangeably refer to the linked account, the IoT device, etc. as the central object of focus (adding to cognitive load). However, 'Feedback' during decoupling of devices was generally present, keeping all users aware (with implications here for users with either primary or secondary perspectives).

5.3.7 Help & documentation. 'Help and documentation' is another notable challenge – like many modern computing devices, instructions and guidance for the novice user are limited. The immediate advice in the boxes with the devices, and the associated App(s), does not mention the full range of *interfaces* that we have assessed here (though this information is available publicly online). Compounding the lack of documentation is the reliance on a user to have the will to invest speculatively in searching locally and online for helpful features and guidance on how to use them. Devices and their features 'speak the user's language' only up to a point, beyond which non-novice features leverage a different family of terms. Other research found that one person may have more knowledge than others in a household [62]. Life disruptions such as domestic violence can disrupt technology maintenance practices, especially if a person acting maliciously is also the person managing devices and their use [61]. In our work we find that there is an 'opportune moment' [57] for configuring security, which may in fact not be easily accessible to those assumed to be aware of it.

5.4 Summary

Here we summarise the findings, revisiting the overarching Research Questions (Section 1). We also broadly consider how various stakeholders can coordinate support, recognising intervention points such as those described by the 'Tech vs Abuse' (UK) initiative [76]: awareness of abuse, finding the right information at the right time, accessing (effective, real-time) support, and recovery.

Heuristic violations were generally clustered across specific heuristics (Section 2.4) or within a particular phase of abuse (Section 3.3). This suggests that interventions and support can be targeted (RQ1). For many heuristics across most phases, we did not identify usability violations (RQ3). In the multi-user connected environment, a lack of violations also means that usability does however benefit a perpetrator as much as a survivor; the path to safety is not straightforward.

Where there are violations of a usability heuristic across all phases of abuse, this implies that care should be taken to either change the way IoT devices operate, or target the heuristic when developing interventions. That 'Consistency' was a problem across phases implies that advice may need to be made specific to devices (through involvement with policymakers, but also device makers, and potentially retail and community touch-points). Relating to RQ2, this becomes a challenge if devices and device combinations are expected to scale, pointing to a need for standardisation. Ur et al. [78] found inconsistent behaviour between functionally similar devices when studying a set of three smart devices (a smart lock, bathroom scale, and lighting system).

Similarly, 'Help & Documentation' would require clear signposting and access to actionable advice (through not just online, but also local communication channels), though this risks also being visible to a perpetrator (RQ3). As a consequence, on-the-ground stakeholders such as local law enforcement, and statutory and voluntary services, may have a need to be able to act or reach the survivor quickly (even where minor usability problems impose delays), through any of the *interfaces* or in-person. There may also need to be support from technology specialists, to determine how devices have been co-opted for tech-abuse [30].

That the 'Feedback' heuristic sees violations across most phases then signals a point of caution (RQ2). If activity notifications are not produced, this may give a survivor a chance to enact Escape. With this, support services would need skills – or access to skills – to be able to support a transition to 'Life Apart', especially if the survivor has mobile or smart devices that were once shared. That there is feedback in the 'Configuration' phase is dampened by the potentially alien nature of IoT terminology to novice users ('User's Language'), informing RQ2. This may make diagnosis of problems difficult, potentially requiring technical experts to have a role in the process of leaving an abusive environment. However, this also means that a survivor may not be aware of anything a perpetrator has done to configure or monitor a device, especially across the various interfaces (an existing challenge in mitigating tech-abuse). Feedback is then one point where the definition of usability must be considered carefully (RQ2), so as not to burden the survivor with cognitive load (in ascertaining the configuration of the device ecosystem). Providing support here begins with the design and usability of the devices and their features, requiring consideration of how connected devices and services interact with each other around interpersonal interactions (RQ1), although designing to prevent abuse while enabling legitimate usage is potentially challenging [87].

Prior research has aimed to classify IoT devices according to technical capabilities, to provide users with security and privacy guidance for the devices they purchase (e.g., [44]). Home users keen to connect IoT devices and discover the capabilities of their smart home may find that protective settings limit that potential. It may also be seen by others in the shared home environment as over-cautious or divisive, especially if routinely checking a range of different interfaces (RQ2). This potentially requires a cultural shift toward respecting another person's digital privacy and conveying protective measures as normal, while also working with manufacturers to ensure the immediate security of devices (RQ1).

Regarding the accessibility of devices and support, people may receive or follow bad advice which leads to negative experiences [64], or only seek help after such experiences. Within this is a suggestion to explore new channels for delivering good advice. It can also

be the case that participants feel exploited – rather than served – by IoT devices, or that these devices are seen as exclusive [32], perceptions which can impact willingness to engage with them.

6 DISCUSSION

To revisit the phases of abuse as stages of use (RQ1) (Section 1), users are directly notified of some events, but generally 'Feedback' is inconsistent. Existing work suggests that IoT users need to gain security awareness and competences. What is currently missing from the conversation is support for a user's *risk awareness*, to know *when* to apply what they know, especially in a dynamic situation where some security tasks may have been delegated to others. Interplay between risk perception and security awareness has been examined in corporate settings [5].

For specific usability issues (RQ2), a user of an IoT device may need a running memory of the current configuration state of their devices, to know if it has changed (for lack of direct notification of state changes). The assumption of a 'smart home' is perhaps overloaded, as a place where agreement on device configuration choices emerges naturally and is known to all concurrent users. If cross-device functionality is not standardised ('Consistency' heuristic), general advice could be provided but expertise with one device may not translate to another.

A lack of usability violations for both primary and secondary users has implications, for what 'usability' ought to be in a shared environment with tensions between users of the same devices. There must be *fairness* in the use of shared, connected devices [43], including that a person will not suffer as a result of circumstances outside of their control.

The person who chooses, configures, and manages smart home devices may have power over others in a shared space because of this [26]. Conversely, other users may have less interest in managing them, or less technical knowledge. A user may then have comparatively limited access if they are not the device 'installer', where control over shared devices may exacerbate an existing power imbalance and climate of abuse [87]. A sense of fairness may then be regarded as a person's natural *claim* on access [59] rather than their technical knowledge.

The analysis informs whether moving on to 'Life Apart' is a case of discarding all devices and accounts, or whether connections can be undone and reshaped; current advice might be to discard computing devices, such as smartphones, and start anew, further impacting the survivor. We found that a subset of interfaces supported 'disentanglement', but that issues in existing research around online monitoring and control may remain.

6.1 Other areas of application

Insider threat research considers situations where an attacker uses the same infrastructure as a defender. This immediately suggests that insider threat research (e.g., [70]) – normally considered in a corporate environment – could be re-purposed to inform support for survivors of tech-abuse. In a connected, consumer device environment, individual devices may be shared by users, who may be using legitimate device features (in a 'UI-bound' manner). Of note from insider threat research is that, for instance, the monitoring of all system users can erode trust among well-meaning users.

Our approach can also be applied to research of 'smart' cities (communities of users), and responses to soft security behaviour 'nudges' [9] and 'prods' [65] (where deployment ought to avoid harmful side-effects to well-meaning users). It may be that the design of devices and shared spaces can be leveraged as a means to limit (cyber) crimes, such as through the Security Function Framework [18], which explicitly considers the objectives for a security (or securing) product to uphold *desire* and *social responsibility* (hygiene) expectations.

6.2 Research approach – risks and benefits

Referring to the principles of the Menlo Report [15] and ACM Code of Ethics 2018 [3], a focus in this study has been on *respect for those persons* [15] who could be negatively affected by misuse of smart devices; the devices we have analysed are popular and widely available for purchase (and hence accessible to the public, defenders, and perpetrators of abuse), and used increasingly in homes. Given the sensitivity of the research area, we decided that open disclosure of exactly what we did and what the outcomes were was not appropriate, restricting what we share openly as per considerations around potential misuse [22, 51]. Perpetrators of tech-abuse may misuse legitimate features, where here we do not wish to document how misuse may be enacted. There are challenges in preventing misuse while enabling benign use [87], and in sharing evidence between stakeholders in security research [73]. Rather, we aim to encourage and engage in dialogue with stakeholders who can use results to identify countermeasures (such as policymakers, device manufacturers, support services, and others as mentioned in Section 5.4).

In this work, one aim is to motivate the communities of research and practice to develop capabilities to respond to these challenges. The potential benefits of subsequent research may however need to reconsider the need to give shape to foundational results in order to build on them.

Serving *beneficence* [15], existing research suggests that a collective capability to analyse and respond to shared device threats does not exist currently, where we argue that it should be developed (including a capacity to anticipate unintended consequences of security measures when deployed in a shared smart device ecosystem). In other areas of research there is a similar need to identify and bring together stakeholders, such as when analysing datasets of illicit origin [77]. At this juncture, in such a case where the interest of different groups conflict, we consider *justice* [15] and err toward prioritising the needs of those less advantaged to mitigate harms [3] and respect related social needs [3] and *public interest* [15].

The above are considerations for the tech-abuse case study we explored here. Other applications of the shared device threat analysis approach ought to revisit the above principles. For instance, if researchers analysed devices which are confirmed to no longer be in active use or relate to current devices in any way, their assessment of risks may differ in terms of where user groups are vulnerable to threats which they may otherwise not know about. Alternatively, where we have reported results in a comparatively subjective manner by way of usability principles, other indirect but useful reporting mechanisms could be developed.

7 RELATED WORK

The interplay between security and usability has been considered as part of principled analysis in a number of ways. Atzeni et al. [4] developed attacker personas, based on available information about attackers; the data could then be structured to explore an attacker's capacity to learn about an organisation and launch insider attacks. Personas supported workshop-based discussions between technically-knowledgeable stakeholders. We explore a user's capacity to undermine the security and privacy of others in the same device ecosystem through legitimate controls.

Sindre et al. modelled misuse cases [71], distinguishing between a legitimate use case limiting the capability to misuse a system, and vice versa. The authors posit that lightweight descriptions sufficiently describe simple attacks. We find that 'UI-bound' IoT tasks map to relatively basic activities which can nonetheless impact concurrent users. Similarly, He et al. [31] describe how users of the same IoT devices may have competing expectations around the access rights that other users should have, which suggests a need to classify use and misuse within the same shared system.

Kainda et al. [38] consider specific properties of usability and security in tandem (such as satisfaction and efficiency, and attention and vigilance, respectively). The accompanying framework includes steps to identify usage and threat scenarios. We consider that the two may be the same, but with differing implications for different users within a shared device ecosystem. The authors consider external motivators of threats; we consider the role of external motivators and actors for limiting harm, and the development of interventions which do not themselves introduce or facilitate harm. In other work [39], the authors assessed the implications of security failures within group-based security bootstrapping tasks. 'Sum-of-efforts' security is considered; rather than collective efforts, we are concerned with individuals impacting the security and safety of another individual in a multi-device environment.

Focusing specifically on tech-abuse, Emms et al. [20] note that the use of digital technologies can unknowingly leave signs of use, which a perpetrator might see. IoT devices may similarly produce a trail of activity visible in the connected environment; this is an example of needing to consider user capabilities, as legitimate users would ideally not be required resort to stop using a device to preserve their security. Loi et al. [44] systematically analyse the security and privacy of emerging IoT devices towards informing consumers, focusing on technical capabilities (such as confidentiality of transmissions to an app or server). The authors further argue that IoT devices will become increasingly diverse and complex.

In the practitioner space, Mozilla maintain an ongoing review of consumer IoT smart home devices, through the '*Privacy Not Included' initiative [50]. Devices ranging from toys, to wearables and health devices, are rated against a 'Creepy-o-Meter'. A device's rating is informed by qualities such as 'can I control it?' and 'what could happen if something goes wrong?'. At the time of writing, few devices were deemed to be 'not creepy'; factors such as these may impact how approachable IoT devices are perceived to be. Emami-Naeini et al. [52] engaged more than 1,000 participants through IoT-related scenarios, to discern privacy preferences. Preferences were diverse, influenced by contextual factors such as the data being accessed, and who it is shared with. An environment of abuse may result in IoT preferences changing dramatically (such as a survivor wishing to 'disentangle' online accounts); we explore where support for preference changes may or may not introduce further harms.

Harbers et al. [28] assess IoT functionality across a series of 'layers', including physical interactions with IoT devices. These layers contribute to the complexity of IoT systems which stakeholders must consider. The authors argue that the rapid development of IoT capabilities creates a perpetual knowledge gap for maintaining device security; our work begins to characterise the potential implications of such a knowledge gap in use of shared consumer devices. From interviews with 40 owners of IoT devices, Williams et al. [84] argued that a lack of familiarity with complex IoT devices can lead users to neglect device security, where this further compounds the need for support to mitigate IoT-facilitated harms.

Kaaz et al. [37] explore the 'plug-and-play' capacity of IoT devices, toward identifying misconceptions and directions for where supporting guidance can close gaps in being able to skilfully configure IoT devices. A user study found that instructions were deceptively simple, that installing relevant apps was a barrier, and that configuring devices and networks imposed context-switches and cognitive load upon users (all before considering that another user may act to undermine these efforts).

8 CONCLUSIONS

IoT-facilitated tech abuse is an emerging phenomena that requires the attention of the research community as much as the practitioner and policy community. In a dynamic of abuse, a survivor may need to hide their activity from another user, or be supported to create opportunities to mitigate and escape harm. Here we explore these complexities, focusing on the usability of security-related device features in an IoT ecosystem, pointing to how it can be managed to develop security-related interventions.

We adapted existing usability analysis methods to present a novel approach to systematically describing and assessing *mechanisms of connectedness* in shared IoT devices, and their security implications. This helps us to understand how smart consumer device behaviour can impact users of a shared space under *internal threats*, specifically the potential for IoT-facilitated tech-abuse.

The authors do not assert that the evaluation is complete, in terms of whether features are safe to use or are certain to create harm. The work will be broadened to include a larger range of devices and device connections. We envisage that such a capability is required, to systematically analyse consumer IoT devices individually and in combination, having here analysed a small set of individual devices in isolation and with default settings.

Outcomes are of use for researchers, but can also be communicated to frontline support services and technical bodies. Our work points more broadly to the compound need for *fair usability* in a shared connected environment, to resolve technology-facilitated problems in the shared space, where usable devices and features cannot necessarily be relied on to achieve this.

Ongoing work will explore the implications of IoT consumer device functionality for specific user communities, and other forms of abuse relating to specific groups, be it gender-based, or otherwise based on culture, tech literacy, or other attributes. Current practice

implies that specific considerations and design decisions may be required for support to be effective in different contexts[7].

ACKNOWLEDGMENTS

The authors would like to thank the attendees of our engagement workshops, and the UCL STEaPP researchers who helped run the events (Kruakae Pothong, Ellie Cosgrave, and Zoe Henderson). We also thank the attendees and scribes of NSPW 2019, and our NSPW shepherds, for guidance. The UCL "Gender and IoT" project is funded by grants from the UCL Social Science Plus+ scheme, UCL Public Policy, PETRAS IoT Research Hub, and the NEXTLEAP Project (EU Horizon 2020 Framework Programme for Research and Innovation, H2020-ICT-2015, ICT-10-2015, grant agreement No. 688722). Jonathan Spring provided invaluable feedback on the methodology. The authors thank George Danezis for his support.

REFERENCES

[1] Anne Adams and Anna L Cox. 2008. Questionnaires, in-depth interviews and focus groups. *Research Methods for Human Computer Interaction* (2008), 17–34.
[2] Budi Arief, Kovila PL Coopamootoo, Martin Emms, and Aad van Moorsel. 2014. Sensible privacy: how we can protect domestic violence survivors without facilitating misuse. In *Proceedings of the 13th Workshop on Privacy in the Electronic Society*. ACM, 201–204.
[3] Association for Computer Machinery. 2018. ACM Code of Ethics and Professional Conduct. https://www.acm.org/code-of-ethics. Accessed: 08-11-2019.
[4] Andrea Atzeni, Cesare Cameroni, Shamal Faily, John Lyle, and Ivan Fléchais. 2011. Here's Johnny: a methodology for developing attacker personas. In *2011 Sixth International Conference on Availability, Reliability and Security*. IEEE, 722–727.
[5] Odette Beris, Adam Beautement, and M Angela Sasse. 2015. Employee rule breakers, excuse makers and security champions: Mapping the risk perceptions and emotions that drive security behaviors. In *Proceedings of the 2015 New Security Paradigms Workshop (NSPW)*. ACM, 73–84.
[6] Nellie Bowles. 2018. Thermostats, Locks and Lights: Digital Tools of Domestic Abuse. https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html. Accessed: 03-07-2019.
[7] Irina Brass, Leonie Tanczer, Madeline Carr, Miles Elsden, and Jason Blackstock. 2018. Standardising a moving target: The development and evolution of IoT security standards. *Living in the Internet of Things: Cybersecurity of the IoT* (2018).
[8] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.
[9] Pamela Briggs, Debbie Jeske, and Lynne Coventry. 2017. Behavior change interventions for cybersecurity. In *Behavior Change Research and Theory*. Elsevier, 115–136.
[10] Tara Capel, Dhaval Vyas, and Margot Brereton. 2017. Women in Crisis Situations: Empowering and Supporting Women Through ICTs. In *IFIP Conference on Human-Computer Interaction*. Springer, 64–84.
[11] Lizzie Coles-Kemp and René Rydhof Hansen. 2017. Walking the line: The everyday security ties that bind. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*. Springer, 464–480.
[12] Kovila P.L. Coopamootoo, Thomas Gross, and M. Faizal R. Pratama. 2017. An Empirical Investigation of Security Fatigue: The Case of Password Choice after Solving a CAPTCHA. In *Learning from Authoritative Security Experiment Results (LASER 2017)*. USENIX Association, 39–48.
[13] Pia S de Boer, Alexander JAM van Deursen, and Thomas JL van Rompay. 2019. Accepting the Internet-of-Things in our homes: The role of user skills. *Telematics and informatics* 36 (2019), 147–156.
[14] Department for Digital, Culture, Media & Sport (DCMS), UK. 2018. Code of Practice for Consumer IoT Security. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security (Accessed 15/11/2019)
[15] David Dittrich, Erin Kenneally, et al. 2012. The Menlo Report: Ethical principles guiding information and communication technology research. *US Department of Homeland Security* (2012).
[16] Heather Douglas, Bridget Harris, and Molly Dragiewicz. 2019. Migrant women are particularly vulnerable to technology-facilitated domestic abuse. https://theconversation.com/migrant-women-are-particularly-vulnerable-to-technology-facilitated-domestic-abuse-110270. Accessed: 03-07-2019.
[17] Jide S Edu, Jose M Such, and Guillermo Suarez-Tangil. 2019. Smart Home Personal Assistants: A Security and Privacy Review. *arXiv preprint arXiv:1903.05593* (2019).
[18] Paul Ekblom. 2012. The security function framework. *P Ekblom (Ed.), Design Against Crime: Crime Proofing Everyday Objects. Crime Prevention Studies* 27 (2012).
[19] Jon D Elhai, Jason C Levine, and Brian J Hall. 2017. Anxiety about electronic data hacking: Predictors and relations with digital privacy protection behavior. *Internet Research* 27, 3 (2017), 631–649.
[20] Martin Emms, Budi Arief, and Aad van Moorsel. 2012. Electronic footprints in the sand: Technologies for assisting domestic violence survivors. In *Annual Privacy Forum*. Springer, 203–214.
[21] ENISA. 2017. Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot (Accessed 15/11/2019)
[22] European Commission (Directorate - General for Migration and Home Affairs) (Directorate-General for Research and Innovation). [n.d.]. Guidance note - Potential misuse of research. http://ec.europa.eu/research/participants/data/ref/h2020/other/hi/guide_research-misuse_en.pdf (Accessed 06/04/2019)
[23] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2017. Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders. *PACM: Human-Computer Interaction: Computer-Supported Cooperative Work and Social Computing (CSCW) Vol* 1 (2017).
[24] Diana Freed, Jackeline Palmer, Diana Minchala, Karen Levy, Thomas Ristenpart, and Nicola Dell. 2018. "A Stalker's Paradise": How Intimate Partner Abusers Exploit Technology. In *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*. ACM, 667.
[25] Silvia Gabrielli and Anthony Jameson. 2009. Obstacles to option setting: Initial results with a heuristic walkthrough method. In *IFIP Conference on Human-Computer Interaction*. Springer, 600–603.
[26] Christine Geeng and Franziska Roesner. 2019. Who's In Control?: Interactions In Multi-User Smart Homes. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 268.
[27] "Gender and IoT" Research Team. 2018. The Implications of the Internet of Things (IoT) on Victims of Gender-Based Domestic Violence and Abuse (G-IoT) - Policy Leaflet. https://www.ucl.ac.uk/steapp/sites/steapp/files/giot_policy_.pdf (Accessed 15/11/2019)
[28] Maaike Harbers, Mortaza Bargh, Ronald Pool, Jasper Van Berkel, Susan Van den Braak, and Sunil Choenni. 2018. A Conceptual Framework for Addressing IoT Threats: Challenges in Meeting Challenges. In *Proceedings of the 51st Hawaii International Conference on System Sciences*.
[29] Eric Hatleback and Jonathan M Spring. 2014. Exploring a mechanistic approach to experimentation in computing. *Philosophy & Technology* 27, 3 (2014), 441–459.
[30] Sam Havron, Diana Freed, Rahul Chatterjee, Damon McCoy, Nicola Dell, and Thomas Ristenpart. 2019. Clinical computer security for victims of intimate partner violence. In *28th USENIX Security Symposium (USENIX Security 19)*. 105–122.
[31] Weijia He, Maximilian Golla, Roshni Padhi, Jordan Ofek, Markus Dürmuth, Earlence Fernandes, and Blase Ur. 2018. Rethinking access control and authentication for the home Internet of Things (IoT). In *27th USENIX Security Symposium (USENIX Security 18)*. 255–272.
[32] Claude PR Heath, Clara Crivellaro, and Lizzie Coles-Kemp. 2019. Relations are more than Bytes: Re-thinking the Benefits of Smart Services through People and Things. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*. ACM, 308.
[33] Nicola Henry and Anastasia Powell. 2018. Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, violence, & abuse* 19, 2 (2018), 195–208.
[34] Phyllis McKay Illari and Jon Williamson. 2012. What is a mechanism? Thinking about mechanisms across the sciences. *European Journal for Philosophy of Science* 2, 1 (2012), 119–135.
[35] Internet Society. 2018. IoT Security for Policymakers. https://www.internetsociety.org/resources/2018/iot-security-for-policymakers/ (Accessed 15/11/2019)
[36] ISO/IEC. 2011. *BS ISO/IEC 25010:2011 - Systems and software engineering. Systems and software quality requirements and evaluation (SQuaRE). System and software quality models.*
[37] Kim J Kaaz, Alex Hoffer, Mahsa Saeidi, Anita Sarma, and Rakesh B Bobba. 2017. Understanding user perceptions of privacy, and configuration challenges in home automation. In *2017 IEEE Symposium on Visual Languages and Human-Centric Computing (VL/HCC)*. IEEE, 297–301.
[38] Ronald Kainda, Ivan Flechais, and AW Roscoe. 2010. Security and usability: Analysis and evaluation. In *2010 International Conference on Availability, Reliability and Security*. IEEE, 275–282.
[39] Ronald Kainda, Ivan Flechais, and AW Roscoe. 2010. Two heads are better than one: security and usability of device associations in group scenarios. In *Proceedings of the Sixth Symposium on Usable Privacy and Security*. ACM.

[7] The need for principled design to address different forms of abuse has been raised in practice, for instance by the UK's Tech vs Abuse initiative [75].

[40] David Kotz and Travis Peters. 2017. Challenges to ensuring human safety throughout the life-cycle of Smart Environments. In *Proceedings of the 1st ACM Workshop on the Internet of Safe Things*. ACM, 1–7.

[41] Kat Krol, Jonathan M Spring, Simon Parkin, and M Angela Sasse. 2016. Towards robust experimental design for user studies in security and privacy. In *The LASER Workshop: Learning from Authoritative Security Experiment Results (LASER 2016)*. 21–31.

[42] Deepak Kumar, Kelly Shen, Benton Case, Deepali Garg, Galina Alperovich, Dmitry Kuznetsov, Rajarshi Gupta, and Zakir Durumeric. 2019. All things considered: an analysis of IoT devices on home networks. In *28th USENIX Security Symposium (USENIX Security 19)*. 1169–1185.

[43] Joseph Galen Lindley, Paul Coulton, Haider Akmal, Duncan Hay, Max Van Kleek, Sara Cannizzaro, and Reuben Binns. 2019. The Little Book of Philosophy for the Internet of Things. https://www.petrashub.org/download/the-little-book-of-philosophy-for-the-internet-of-things/ (Accessed 15/11/2019)

[44] Franco Loi, Arunan Sivanathan, Hassan Habibi Gharakheili, Adam Radford, and Vijay Sivaraman. 2017. Systematically Evaluating Security and Privacy for Consumer IoT Devices. In *Proceedings of the 2017 Workshop on Internet of Things Security and Privacy*. ACM, 1–6.

[45] Isabel Lopez-Neira, Trupti Patel, Simon Parkin, George Danezis, and Leonie Tanczer. 2019. 'Internet of Things': How abuse is getting smarter. *Safe–The Domestic Abuse Quarterly* 63 (2019), 22–26.

[46] Michael Massimi, Jill P Dimond, and Christopher A Le Dantec. 2012. Finding a new normal: the role of technology in life disruptions. In *Proceedings of the ACM 2012 conference on computer supported cooperative work*. ACM, 719–728.

[47] Tara Matthews, Kathleen O'Leary, Anna Turner, Manya Sleeper, Jill Palzkill Woelfer, Martin Shelton, Cori Manthorne, Elizabeth F Churchill, and Sunny Consolvo. 2017. Stories from survivors: Privacy & security practices when coping with intimate partner abuse. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 2189–2201.

[48] Wendy Moncur, Lorna Gibson, and Daniel Herron. 2016. The role of digital technologies during relationship breakdowns. In *Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing*. ACM, 371–382.

[49] Stephanie Moser, Susanne Elisabeth Bruppacher, and Hans-Joachim Mosler. 2011. How people perceive and will cope with risks from the diffusion of ubiquitous information and communication technologies. *Risk analysis* 31, 5 (2011), 832–846.

[50] Mozilla. 2018. *privacynotincluded. https://foundation.mozilla.org/en/privacynotincluded/ (Accessed 15/11/2019)

[51] MRC, BBSRC, and Wellcome Trust. 2015. Managing Risks of Research Misuse. https://mrc.ukri.org/research/policies-and-guidance-for-researchers/managing-risks-of-research-misuse/

[52] Pardis Emami Naeini, Sruti Bhagavatula, Hana Habib, Martin Degeling, Lujo Bauer, Lorrie Cranor, and Norman Sadeh. 2017. Privacy Expectations and Preferences in an IoT World. In *Symposium on Usable Privacy and Security (SOUPS)*.

[53] Jakob Nielsen. 1992. Finding usability problems through heuristic evaluation. In *Proceedings of the SIGCHI conference on Human factors in computing systems*. ACM, 373–380.

[54] Jakob Nielsen. 1994. Enhancing the explanatory power of usability heuristics. In *Proceedings of the SIGCHI conference on Human Factors in Computing Systems*. ACM, 152–158.

[55] Jakob Nielsen. 1994. Heuristic Evaluation. In *Usability Inspection Methods*, Jakob Nielsen and Robert L. Mack (Eds.). John Wiley & Sons, Inc., New York, NY, USA, 25–62.

[56] Ilse Oosterlaken and Jeroen van den Hoven. 2011. ICT and the capability approach. *Ethics and Information Technology* 13, 2 (2011), 65–67.

[57] Simon Parkin, Elissa M Redmiles, Lynne Coventry, and M Angela Sasse. 2019. Security When it is Welcome: Exploring Device Purchase as an Opportune Moment for Security Behavior Change. In *Workshop on Usable Security and Privacy (USEC)*.

[58] Shirley Patton. 2003. Pathways: How women leave violent men. *Partnerships Against Domestic Violence (Commonwealth Government of Australia)* (2003).

[59] Wolter Pieters. 2019. Everything-as-a-Hack: Claims-Making for Access to Digital and Social Resources. In *Proceedings of the 2019 New Security Paradigms Workshop (NSPW)*. ACM.

[60] David Pinelle, Carl Gutwin, and Saul Greenberg. 2003. Task analysis for groupware usability evaluation: Modeling shared-workspace tasks with the mechanics of collaboration. *ACM Transactions on Computer-Human Interaction (TOCHI)* 10, 4 (2003), 281–311.

[61] Erika S Poole. 2014. Is Living With Others A Barrier To Technical Literacy?. In *Proceedings of the 18th International Conference on Supporting Group Work*. ACM, 178–181.

[62] Erika Shehan Poole, Marshini Chetty, Tom Morgan, Rebecca E Grinter, and W Keith Edwards. 2009. Computer help at home: methods and motivations for informal technical support. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 739–748.

[63] Krystalle Ramlakhan. 2019. Abusers tracking victims through technology, shelters say. https://www.cbc.ca/news/canada/ottawa/rise-tracking-monitoring-victims-women-violence-domestic-abuse-ottawa-quebec-outaouais-1.5069744. Accessed: 03-07-2019.

[64] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. 2017. Where is the digital divide?: A survey of security, privacy, and socioeconomics. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*. ACM, 931–936.

[65] Karen Renaud and Verena Zimmermann. 2018. Ethical guidelines for nudging in information security & privacy. *International Journal of Human-Computer Studies* 120 (2018), 22–35.

[66] Paul Roe. 2008. The 'value' of positive security. *Review of international studies* 34, 4 (2008), 777–794.

[67] Corina Sas and Steve Whittaker. 2013. Design for forgetting: disposing of digital possessions after a breakup. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 1823–1832.

[68] Roei Schuster, Vitaly Shmatikov, and Eran Tromer. 2018. Situational Access Control in the Internet of Things. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*. ACM, 1056–1073.

[69] Andrew Sears. 1997. Heuristic walkthroughs: Finding the problems without the noise. *International Journal of Human-Computer Interaction* 9, 3 (1997), 213–234.

[70] George J Silowash, Dawn M Cappelli, Andrew P Moore, Randall F Trzeciak, Timothy Shimeall, and Lori Flynn. 2012. Common sense guide to mitigating insider threats. *Technical Report CMU/SEI-2012-TR-012* (2012).

[71] Guttorm Sindre and Andreas L Opdahl. 2005. Eliciting security requirements with misuse cases. *Requirements engineering* 10, 1 (2005), 34–44.

[72] Jonathan M Spring and Phyllis Illari. 2018. Building general knowledge of mechanisms in information security. *Philosophy & Technology* (2018), 1–33.

[73] Jonathan M. Spring, Tyler Moore, and David Pym. 2017. Practicing a Science of Security: A Philosophy of Science Perspective. In *Proceedings of the 2017 New Security Paradigms Workshop (NSPW 2017)*. ACM.

[74] Leonie Tanczer, Irina Brass, Miles Elsden, Madeline Carr, and Jason J Blackstock. 2019. The United Kingdom's Emerging Internet of Things (IoT) Policy Landscape. *Rewired: Cybersecurity Governance* (2019), 37–56.

[75] Tech vs Abuse (Comic Relief). 2019. Tech vs Abuse: Design Principles. https://www.techvsabuse.info/design-principles (Accessed 15/11/2019)

[76] Tech vs Abuse (Comic Relief). 2019. Tech vs Abuse: Research Findings. https://www.techvsabuse.info/research-findings (Accessed 15/11/2019)

[77] Daniel R Thomas, Sergio Pastrana, Alice Hutchings, Richard Clayton, and Alastair R Beresford. 2017. Ethical issues in research using datasets of illicit origin. In *Proceedings of the 2017 Internet Measurement Conference*. ACM, 445–462.

[78] Blase Ur, Jaeyeon Jung, and Stuart Schechter. 2013. The current state of access control for smart devices in homes. In *Workshop on Home Usable Privacy and Security (HUPS)*. HUPS 2014.

[79] Ersin Uzun, Kristiina Karvonen, and Nadarajah Asokan. 2007. Usability analysis of secure pairing methods. In *International Conference on Financial Cryptography and Data Security*. Springer, 307–324.

[80] Jennifer Valentino-DeVries. 2018. Hundreds of Apps Can Empower Stalkers to Track Their Victims. https://www.nytimes.com/2018/05/19/technology/phone-apps-stalking.html. Accessed: 03-07-2019.

[81] Aad van Moorsel, Martin Emms, Gemma Rendall, and Budi Arief. 2011. *Digital Strategy for the Social Inclusion of Survivors of Domestic Violence*. Technical Report. Citeseer.

[82] Kami Vaniea, Ella Tallyn, and Chris Speed. 2017. Capturing the Connections: Unboxing Internet of Things Devices. *arXiv preprint arXiv:1708.00076* (2017).

[83] Cathleen Wharton, John Rieman, Clayton Lewis, and Peter Polson. 1994. The Cognitive Walkthrough Method: A Practitioner's Guide. In *Usability Inspection Methods*, Jakob Nielsen and Robert L. Mack (Eds.). John Wiley & Sons, Inc.

[84] Meredydd Williams, Jason RC Nurse, and Sadie Creese. 2017. "Privacy is the Boring Bit": User Perceptions and Behaviour in the Internet-of-Things. In *Proceedings 15th International Conference on Privacy, Security and Trust*.

[85] Delanie Woodlock. 2017. The abuse of technology in domestic violence and stalking. *Violence against women* 23, 5 (2017), 584–602.

[86] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security & Privacy Concerns with Smart Homes. In *Symposium on Usable Privacy and Security (SOUPS)*.

[87] Eric Zeng and Franziska Roesner. 2019. Understanding and improving security and privacy in multi-user smart homes: a design exploration and in-home user study. In *28th {USENIX} Security Symposium ({USENIX} Security 19)*. 159–176.

[88] Mary Ellen Zurko. 2005. User-centered security: Stepping up to the grand challenge. In *21st Annual Computer Security Applications Conference (ACSAC'05)*. IEEE.