Can prosuming become perilous? Exploring systems of control and domestic abuse in the smart homes of the future


This version is available from Sussex Research Online: http://sro.sussex.ac.uk/id/eprint/105701/

This document is made available in accordance with publisher policies and may differ from the published version or from the version of record. If you wish to cite this item you are advised to consult the publisher's version. Please see the URL above for details on accessing the published version.

Copyright and reuse:
Sussex Research Online is a digital repository of the research output of the University.

Copyright and all moral rights to the version of the paper presented here belong to the individual author(s) and/or other copyright owners. To the extent reasonable and practicable, the material made available in SRO has been checked for eligibility before being made available.

Copies of full text items generally can be reproduced, displayed or performed and given to third parties in any format or medium for personal research or study, educational, or not-for-profit purposes without prior permission or charge, provided that the authors, title and full bibliographic details are credited, a hyperlink and/or URL is given for the original metadata page and the content is not changed in any way.
Can Prosuming Become Perilous? Exploring Systems of Control and Domestic Abuse in the Smart Homes of the Future

Benjamin Sovacool*, Dylan D Furszyfer-Del Rio and Mari Martiskainen

Science Policy Research Unit, University of Sussex Business School, Brighton, United Kingdom

In what ways can new, emerging digital technologies and energy business models such as “prosuming” become intertwined with troubling patterns of domestic abuse and violence? Domestic violence entails controlling, coercive or threatening behaviours, to gain or maintain power and control between intimate partners or family members regardless of gender or sexuality. The rapid development of digital communication services, smart homes, and digitalization processes such as prosuming create surprising threats related to technology-facilitated abuse. In this empirical study, based on a nationally representative survey of householders (n = 1,032 respondents) and three focus groups with the general public in different locations around the UK (n = 18 respondents), we explore the extent that prosuming technologies, smart grids and smart systems could act as potential enablers of domestic violence or systems of control. We also explore the use of smart systems as possible deterrents and mechanisms to reduce and address domestic violence and provide victim protection and recovery. In doing so, we explore user perceptions and preferences of smart systems, in relation to trust, monitoring, tracking, and surveillance. We finally discuss our results through the themes of duality and policy and provide conclusions with recommendations for further research.

Keywords: domestic violence, smart homes, smart home technologies, gender and technology, sexual exploitation and abuse

1 INTRODUCTION

Access to the Internet is perceived as a key service to gaining efficient access to information (Butler and Abrahart, 1997), guaranteeing economic well-being, advancing social conditions and achieving convenience. Therefore, the Internet is increasingly perceived as a fundamental human right (Sandle, 2016). With this in mind, the number of Internet of things (IoT)1 devices continues to grow rapidly (Mckinsey 2019), and in turn, smart systems have become a prominent area of study. For instance, extensive research has focused on the ability of smart systems to offer enhancements in many areas of life. These range from providing health and assisted living services (Balta-Ozkan et al., 2013), to enhancing users’ comfort and convenience (Sovacool and Furszyfer Del Rio 2020) with an
overall aim of boosting productivity and improving citizens’ well-being (OECD, 2018). In sum, smart devices possess the potential to transform human lives given the wide range of application these technologies offer (Hittinger and Jaramillo 2019).

In the energy arena, smart systems intersect with power networks via the deployment of smart grids, where traditionally, passive consumers are now becoming ‘prosumers’ (Morstyn et al., 2018; Bugden and Stedman, 2021). Prosumers are agents that consume and produce energy (Parag and Sovacool, 2016) and can monitor and share information on their energy usage to influence the operations of power systems (Darby and McKennab, 2012). The deployment of smart systems facilitates the transition towards a prosumers era and enables the integration of new business models such as peer-to-peer trading, electric vehicle-to-grid and demand response (Parag and Sovacool, 2016; Furszyfer Del Rio et al., 2020). However, we argue that with the emergence of smart systems and the entrance of novel business models, there is space to promote negative social interactions and iniquitous dynamics of control.

This paper explores whether smart and digital technologies could 1) act as potential enablers of domestic control and violence, and 2) operate as possible deterrents and mechanisms to mitigate such threats. Based on a nationally representative survey of householders (18 years and over) and three focus groups with the general public in the United Kingdom (UK), we explore users’ perceptions and preferences of smart systems concerning trust, monitoring, tracking, and surveillance. We take this approach given that an increasing number of smart connected products are capable of tracking most users’ activities in real-time (Neff and Nafus, 2016; Wajcman, 2019) and contain features of sharing and storing data which can have added negative implications (Zuboff, 2018; Wachter, 2019).

Unlike Furszyfer et al. (2021), who explored smart systems via the lens of gender, our prime contribution consists in investigating how personal data, privacy and surveillance related issues with prosuming or digitalization could enable practices such as, but not limited to, smart monitoring and stalking, domestic violence, and parental control. To do this, we first offer a review of the literature in Section 2. We then infer connections between surveillance, violence and smart systems rather than directly state them, given our initial research design (see Section 3), and present our results in Section 4. In Section 5, we discuss our results through the themes of duality and sometimes competing functions and emotional reactions, as well as the promise of those technologies for mitigating domestic violence.

**2 REVIEWING LITERATURE ON SMART ENERGY AND HOMES, TECHNOLOGY FACILITATED ABUSE, AND MONITORING**

As both prosuming networks and smart systems become more deeply woven into all aspects of our lives, the discussion around the benefits of such technologies has often focused on values such as comfort, convenience and control (Stengers and Nicholls 2017; Marikyan, Papagiannidis, and Alamanos 2019). Previous research regarding the risks of smart systems has mostly explored users’ privacy (Veliz and Grunewald, 2018; Wachter, 2019), whereas a still unattended area is the potential threats that could result from technology related abuse. These include, for example, smart enabled control of family members (Nansen and Jayemanne, 2016), and even domestic violence (Chatterjee et al., 2018; Freed et al., 2018; Henry and Powell, 2018). On the latter, Stark and Hester (2019) indicate that tech abuse can affect individuals psychologically, physically, sexually, financially and emotionally. To this, the Australian national independent regulator for online safety, (2020) has stated that “Technology-facilitated abuse has become ubiquitous in cases of domestic and family violence. It ranges from low tech—like abusive text messaging—to smart home devices like their TV or fridge to exert fear and control.” Indeed, misusing technology to perpetrate violent acts has been acknowledged as a social and economic global problem (UN Broadband Commission for Digital Development, 2015).

In this research, we work from the premise that digital technologies have historically been gendered by design and association and thus, the “cyberspace cannot escape the social construction of gender [Adams (1996) P. 162].” As such, we argue that other forms of violence towards women may persist. For instance, Cintron (2009) and Citron and Norton (2011), suggest that online social outlets (e.g. Twitter and blogs) represent common grounds to attack women, “destroy their privacy,” and diminish their reputation. In consequence, online public debates have historically been dominated by males (Herring, 1999), with others arguing that the internet has often been a “frightening and toxic place for women” (Amnesty International, 2017), Salerno-Ferraro et al. corroborate this point and argue that women are key targets of violence in online spaces, online gaming and social media (Salerno-Ferraro, Erentzen and Schuller, 2021). For Wajcman, the perception that digitalization is a male-dominated field, is explained by constructing gendered identities and discourses produced simultaneously with technologies (Wajcman 2007). Thus, this suggests that technology and gender relations ought to be approached through a technofeminist perspective, where several dimensions involving material, discursive and social elements are considered to avoid excluding women (Wajcman, 2004).

**2.1 Forms of Technology Facilitated Abuse**

Before moving on to key concepts in technology facilitated abuse, we briefly define domestic violence as “any incident or pattern of incidents of controlling, coercive or threatening behaviour, violence or abuse between those aged 16 or over who are or have been intimate partners or family members regardless of gender or sexuality [Home Office (2013) P 2]”. This could entail but is not limited to any form of psychological, physical, sexual, financial or emotional abuse (Leitão, 2018). Domestic violence impacts people and genders in all social, economic, ethnic, educational and cultural groups (Heise and García-Moreno, 2002), but is particularly wide-spread against women and girls (United Nations, 2018). In 2017, UNOCD (2018) reported that 87,000 women were murdered, of which intimate partners or family members killed around 50,000. In the UK context, charity...
TABLE 1 | Included and excluded terms of technology facilitated abuse.

<table>
<thead>
<tr>
<th>Terms included</th>
<th>Terms excluded</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology facilitated sexual abuse (TFSV)</td>
<td>Dockeying</td>
</tr>
<tr>
<td>Digital dating abuse</td>
<td>Cyberbullying</td>
</tr>
<tr>
<td>Image-based sexual violence</td>
<td>Deep fakes</td>
</tr>
<tr>
<td>Cyber stalking</td>
<td>Digital gaslighting</td>
</tr>
<tr>
<td>Online harassment</td>
<td>Impersonating</td>
</tr>
<tr>
<td>Parental monitoring and control</td>
<td></td>
</tr>
<tr>
<td>Femtech, menstruation and pregnancy</td>
<td></td>
</tr>
</tbody>
</table>

This table also lists terms that have been excluded from our study, and although they are a form of technology facilitated abuse, they are not necessarily linked to domestic violence.

Refuge (2018) has estimated that one in four women have experienced domestic violence in their lifetime, while the Crime Survey for England and Wales reported in 2018 that 8.2% of women and 4% of men had experienced domestic violence (Office for National Statistics, 2019). Certainly, intimate partner violence is a complex issue and, as such, can take different forms, from physical and/or sexual violence with a variety of non-violent control tactics to couples’ arguments that turn into aggression and acts of resisting violence (Johnson, 2011).

Research indicates (Henry and Powell, 2015; Woodlock, 2015; Diana Freed et al., 2018; Parkin et al., 2019), however, that domestic violence cases are on the rise, in part, as abuse facilitated by technology does not require face-to-face encounters between victim² and perpetrator (Marganski and Melander, 2018). Technology facilitated abuse does not recognize borders and boundaries, and its victims often feel hounded, under surveillance and harassed by the abuse on their IoT devices and/or social media (Harris and Woodlock, 2019), since these technologies provide instantaneous communication, they enable quick access to methods of harassment and abuse (Melander, 2010; McManus et al., 2021).

There are many forms of technology facilitated abuse and the rapid development of ICTs generate ever-changing patterns of these (see Table 1). These include technology facilitated sexual violence (TFSV), which uses “cell phones, email, social networking sites, chat rooms, online dating sites, and other communications technologies” to enable rape or sexual assault (Henry, Flynn, and Powell 2020; p 1836). Digital dating abuse, another serious offence, consists of a “pattern of behaviours that control, pressure, or threaten a dating partner using a cell phone or the Internet (Reed, Tolman, and Ward 2016; p 1556)” (see also Hinduja and Patchin 2020). For example, data from England and Wales indicate that dating apps have been linked to more than 500 crimes, and whilst the majority are sex offences, others range from murder and rape to child abuse (Kjellsson, 2016).

²Terminology note: Similar to Henry, Flynn and Powell (2020) we have decided to use the term “victim” in our article over “victim-survivor” although we recognized the latter is favoured when dealing with domestic violence issues. However, we used the term “victim” since in our study uses a number of conjoined terms such as but not limited to “technology-facilitated domestic, cyberstalking, and digital dating abuse”. we have decided to simplify the language by using only the term “victim”.

Image-based sexual abuse entails all forms of the non-consensual creation and/or distribution of private sexual images. These include abusive behaviours beyond “revenge porn”, sexual extortion (or “sextortion”), “upskirting, voyeurism and many other similar forms of sexualised abuse (McGlynn, Rackley and Houghton, 2017)”. Vinopal (2020), found that one in 25 people in the US has had a sexual video or image of themselves shared on the internet without their consent, and about 90% of them were women. However, image-based sexual abuse is not confined to adults only—more than 500 children were victims of such abuse in England and Wales last year (Webb and Weale, 2020), and Keller and Dance (2019) have found that child sexual abuse images have doubled in recent years.

Another prominent form of technology facilitated abuse focuses on cyberstalking, which involves the use of digitally connected devices to participate in a “pattern of repeated behaviour that causes the victim to fear for his or her safety (Nobles et al., 2014; pg 988),” also potentially affecting victims’ creativity, concentration, and performance (Holland et al., 2020). Cyberstalking involves using hidden webcams, GPS devices, and spyware to monitor victims’ activities, exert controlling behaviours (Reyns, 2019), and contact the victim under anonymity through fake online profiles (Smoker and March 2017). In comparison to other forms of stalking, cyberstalking victims are more likely to be intimate partners (Cavezza and McEwan, 2014). Linked to cyberstalking is online harassment, a complex concept that varies in expression and severity (Jones, Trott and Wright, 2020) from hateful insults and death threats to humiliating and/or unwelcome conduct of sexual nature (Henry and Powell, 2017; Vil, 2020). Although this problem began with the arrival of the internet, it is pervasive and growing (Anderson, 2017; Vil, 2020), with implications affecting the victims and wider communities when sharing the victim’s identity traits (Nadim and Fladmoe, 2019).

2.2 Parental Monitoring and Control
Children born in connected homes tend to be very conscious of their need for privacy (Leaver, 2017). Particularly, in terms of what they share with their parents and family, rather than what they share with the outside world (Boyd, 2014). Surveillance technologies can create anxiety and hypervigilance (Monahan, 2010) without necessarily increasing children’s health and safety (Hasinoff, 2017). Research also indicates that surveillance and tracking technologies within families may lead to a lack of trust and a reduction in children’s independence and skills to evaluate and respond to risk in public places (Mayer, 2003; Fox, Osborn and Warber, 2014). Research, indicates that children’s use of ICTs and online navigation is often negotiated in complex and nuanced ways (Livingstone and Sefton-Green, 2016). From an infants’ perspective, Ghosh et al., note, after reviewing 736 reviews of 37 mobile online safety apps, that children’s ratings towards monitoring apps were significantly lower than those from parents, with 76% of children’s reviews giving apps a one star. Children, in their study, felt that the apps were restrictive and invasive of their privacy (Ghosh et al., 2018).
Risks, however, are not limited to power dynamics but also practices of data misuse (Holloway, 2019). Children’s wearables (i.e. Owlet) can collect intimate private data about biological activities, oxygen levels, sleeping patterns and children’s peace of mind (Leaver, 2018). These devices are not certified as medical tools (King, 2014) and support the idea that good parenting requires data surveillance practices as a form of care without parents knowing that biometrics infant data is being recorded and monetized. Under these contexts, Grimes (2014) calls for critical awareness of the ideological and political dimensions of infants’ technologies.

### 2.3 Femtech and Menstrual/Health Surveillance

Our final category of literature discusses a class of technology known as "femtech." In the context of smart systems, both Google Play Store and iTunes Store display countless numbers of pregnancy and menstruation-related apps. There is little doubt this market is on the rise, with femtech products and services valued at $17 billion in 2018 and estimations suggesting this market will increase to $50 billion by 2025 (Statista, 2020). Johnson (2014) indicates that pregnancy apps belong to the datafication space contemplating pregnancy as “an administrative and calculable activity, valuing data over subjective experiences and changing the meaning of what is be a mother (2014 p. 346).”. Moreover, research indicates that pregnancy apps have failed in protecting users’ data and their records with information being sold to third parties (Bert et al., 2015). Leaver (2017), in a similar vein, notes that leading pregnancy apps (i.e. Glow) have several vulnerabilities where third parties could access private/intimate information.

Monitoring the health of users in domain of smart homes is not limited to apps. For instance, smart health devices (i.e. Withings Wireless Blood Pressure Monitor or Beddit) could retrieve users’ private data and share it with brokers for profiling and advertising purposes. Such practices contribute to inform decisions and “punish.” users by insurance companies (Furszyfer Del Rio et al., 2020) leading, to some arguing that "smart systems have shifted society from one of disciplined to one of control [having] a normative effect on producing ‘good’ household occupants (Maalsen and Sadowski 2019 p.123 p.123).”.

### 3 MIXED METHODS RESEARCH DESIGN

Our sources of primary data for the study were twofold: a nationally representative survey (with quantitative and qualitative questions) distributed in the United Kingdom, alongside three focus groups. To be clear, both of these instruments were empirical, and had the advantage of collecting data inductively in a grounded manner (rather than nudging respondents or connecting our questions explicitly to any sort of dominant conceptual theory or framework). Figure 1 visually depicts our research design.

Our survey instrument was built off earlier work examining user perceptions of smart homes conducted by Hargreaves and...
Wilson (2017) and Wilson et al. (2015). It was designed to take 10–15 min to complete, and it consisted of twenty questions across four sections. The first section explored the socioeconomic and demographic attributes of respondents. The second section investigated adoption patterns and knowledge of smart home technologies, including smart energy systems and prosuming elements such as peer-to-peer trading or home energy management. The third section examined preferences in smart technology as well as trust and perceived risks. The fourth had open-ended questions asking respondents to share experiences about smart homes and their willingness to be contacted for future research. Most questions used a 5-point Likert Scale (1 = strongly disagree, 5 = strongly agree), with the survey implemented online by a market research company, Dynata, using a respondent panel representative of the UK household population (homeowners and those who rent). Dynata scripted an online version of the survey instrument using their proprietary software. Once checked by the research team, Dynata sent unique person-specific links to the survey to individuals in their respondent panel who have agreed previously to take part in survey research in exchange for incentives. The sampling frame consisted of householders, in the UK, who had to be over the age of at least 18 years old.

A total of 166 respondents were screened out based on quality checks. These quality checks included ‘flak-liners,’ straight-line responses on blocks of questions; ‘rushers,’ those who gave incomplete, contradictory or unrealistic responses (e.g., the respondent who claimed to have 99 children); and ‘speeders,’ those who had unrealistically fast survey completion times. The final sample comprised 1,032 respondents.

To triangulate the findings from the survey, we also conducted three focus groups in the last quarter of 2019 across London (n = 7), Greater Manchester (n = 4), and Surrey (n = 7). This included two urban locations (London and Surrey) and one rural (Manchester). The Focus Groups were organized and managed by a separate market research company, YouGov. The focus

### Table 2: Demographic Attributes of Focus Groups in London, Manchester, and Surrey (n = 18). Source, authors.

<table>
<thead>
<tr>
<th>Focus group 1</th>
<th>London (urban)</th>
<th>Focus group 2</th>
<th>Greater Manchester (Rural)</th>
<th>Focus group 3</th>
<th>Surrey (Rural)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Age</td>
<td>Gender</td>
<td>Ethnicity</td>
<td>Social grade</td>
<td>Gross household income</td>
<td>Smart devices owned</td>
</tr>
<tr>
<td>18</td>
<td>Female</td>
<td>White and Black African</td>
<td>B</td>
<td>£60,000 to £69,999 per year</td>
<td>1</td>
</tr>
<tr>
<td>21</td>
<td>Female</td>
<td>Chinese</td>
<td>C1</td>
<td>£10,000 to £14,999 per year</td>
<td>1</td>
</tr>
<tr>
<td>24</td>
<td>Female</td>
<td>White and Asian</td>
<td>C1</td>
<td>£100,000 to £149,999 per year</td>
<td>1</td>
</tr>
<tr>
<td>54</td>
<td>Female</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>E</td>
<td>Prefer not to answer</td>
<td>3</td>
</tr>
<tr>
<td>56</td>
<td>Male</td>
<td>Any other ethnic group</td>
<td>D</td>
<td>£20,000 to £24,999 per year</td>
<td>4</td>
</tr>
<tr>
<td>62</td>
<td>Male</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>C1</td>
<td>£10,000 to £14,999 per year</td>
<td>1</td>
</tr>
<tr>
<td>73</td>
<td>Male</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>A</td>
<td>£50,000 to £59,999 per year</td>
<td>3</td>
</tr>
<tr>
<td>66</td>
<td>Male</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>C1</td>
<td>£10,000 to £14,999 per year</td>
<td>1</td>
</tr>
<tr>
<td>65</td>
<td>Male</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>B</td>
<td>£35,000 to £39,999 per year</td>
<td>4</td>
</tr>
<tr>
<td>73</td>
<td>Male</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>C2</td>
<td>£45,000 to £49,999 per year</td>
<td>2</td>
</tr>
<tr>
<td>59</td>
<td>Female</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>B</td>
<td>Prefer not to answer</td>
<td>2</td>
</tr>
<tr>
<td>21</td>
<td>Male</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>B</td>
<td>£100,000 to £149,999 per year</td>
<td>5</td>
</tr>
<tr>
<td>29</td>
<td>Male</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>A</td>
<td>Prefer not to answer</td>
<td>1</td>
</tr>
<tr>
<td>33</td>
<td>Male</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>A</td>
<td>£70,000 to £99,999 per year</td>
<td>5</td>
</tr>
<tr>
<td>40</td>
<td>Female</td>
<td>Any other Mixed/Multiple ethnic background</td>
<td>E</td>
<td>£35,000 to £39,999 per year</td>
<td>4</td>
</tr>
<tr>
<td>49</td>
<td>Female</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>B</td>
<td>Prefer not to answer</td>
<td>3</td>
</tr>
<tr>
<td>52</td>
<td>Male</td>
<td>Arab</td>
<td>B</td>
<td>£100,000 to £149,999 per year</td>
<td>2</td>
</tr>
<tr>
<td>58</td>
<td>Male</td>
<td>English/Welsh/Scottish/Northern Irish/British</td>
<td>D</td>
<td>£20,000 to £24,999 per year</td>
<td>1</td>
</tr>
</tbody>
</table>
groups lasted 90 min and involved a mix of different demographic respondents with the details summarized in Table 2. The focus groups followed a similar structure to the survey, examining general knowledge of smart home technologies, experience and usage patterns, perceived benefits and disadvantages, trust, and values. Even though they were recorded and fully transcribed by YouGov, at least one member of the research team observed all of the focus groups.

We analysed our data using SPSS to produce descriptive statistics on our quantitative data, which was supported by inductive thematic analysis of the qualitative data from focus groups and the survey. To ensure anonymity, focus group participants are referred to in our results as follows: London male (FGLM), London female (FGLF); Manchester male (FGMM), Manchester female (FGMF); Surrey male (FGSM) and Surrey female (FGSF). The survey respondents are reported as male/female and respondent number (e.g. MXX, FXX).

Our study has some limitations, mainly the way our survey and focus group questions were designed. Our study was mostly focused on the general risks and benefits smart systems. Therefore, we did not directly ask about abuse or domestic violence, whether participants had experienced technology abuse. Given the sensitivity of this topic, we did not think that it was appropriate to ask about it among a more general survey on smart systems or to raise it as a question in a public focus group setting.

4 RESULTS: VIOLENCE, STALKING, SURVEILLANCE AND PRIVACY IN THE SMART PROSUMING HOME OF THE FUTURE

This section presents our results that fall into the following themes: knowledge as an enabler of domestic violence; smart monitoring and stalking; parental control and surveillance of children; femtech, menstruation and pregnancy.

4.1 Knowledge as an Enabler of Domestic Violence

Our first question explores users’ knowledge of smart systems. Here, we asked survey respondents: How much would you say you know about smart systems? We were interested in participants’ answers in this area since being knowledgeable regarding the use of smart systems may facilitate perpetrators tools to enact cyber abuse or victims to respond to it. For instance, Dimond et al. (2011) indicate that victims of technology abuse felt they were less tech savvy than their abusers. Whilst Freed et al. (2018), show that due to victims’ lack of knowledge, abusers can typically access victims’ digital accounts and devices and use them to control them. We argue that smart systems that undermine victims’ data, privacy, and autonomy should raise serious surveillance concerns related to cyberstalking and even micromanagement.

Our results indicate that most men 60.5% have a good idea to a very good idea of what smart systems are, in contrast to 49.2% of women (see Figure 2). Based on the evidence presented above and findings from Dimond et al. (2011) and later work by Chatterjee et al. (2018), female victims of domestic violence felt that they were less tech savvy than their abusers. We infer from our results that women could be in a more vulnerable position than men. Particularly, since many female participants in our survey stated, for example: “I have very little experience of smart home technologies.” (F288) and “I haven’t used any” (F307). In one of our focus groups, a female participant (FGMF) stated that “I don’t use any smart stuff for anything” when discussing smart systems used for energy monitoring. In a further discussion on whether systems were gendered, one female participant noted that they were “caveated with boys and toys.” (FGSF). More specifically, lack of knowledge was mentioned by one male focus group participant when discussing potential surveillance equipment such as cameras in the house: “I think there are issues that could arise especially in unhealthy relationships where one person is more tech savvy than the other. You don’t know quite what monitoring equipment they might be putting on, let’s say, the bedroom or even the bathrooms.” (FGSM).

However, lack of knowledge not only remains on the victims’ side. A growing body of research (Chayn, 2017; Raptis et al., 2017; Bowles, 2018; Lopez-Neira et al., 2019) suggests that the deficient expert knowledge needed to advise victims about safety and security along with the lack of resources in the legal framework. Due to the lack of expertise in this area, pressure is placed on victims to resolve issues, many of whom feel that they do not possess the knowledge to identify, cope or manage technology abuse.

Indeed, in our own focus groups, participants raised serious concerns regarding lack of knowledge from manufacturers. For instance, FGLM commented: “If you are not tech savvy, you are stuck with the problem until helpdesk decides to help you and sometimes, they do not have an immediate remedy to your problem. There are other worse cases where helpdesk do not even know how to fix your problem”. FGSM elaborated that “I’m tech savvy myself and huge believer of this technology, I installed all the cameras in my house and I can control everything from my phone... unfortunately, as many of these technologies are new and they keep having endless new updates, customer service will not have an answer to all of our problems”. Other male and female participants also noted how these technologies are not easy-to-use, are hard to set-up, and how lack of expertise from manufacturers could lead to trouble. On these subjects, focus group participants stated: “frankly, none of them are easy to set up. I am a geek, and none of them work in the way that they promise they will.” (FGSM) and “it is too complex for some people to contemplate and set up” (FGSM). In our survey, one respondent emphasised that smart systems were “incredibly complex to set up.” (F977).

4.2 Smart Monitoring and Stalking

As shown in Figure 3, women and men have different views regarding smart systems used for monitoring. Our findings indicate that women have a stronger preference for smart systems compared to men to monitor aspects related to health, energy/heat use, household security, entertainment preferences, young children, elderly/ill, household objects, clothing/laundry,
food/diet, pets, financial history, menstruation and pregnancy and family members. Men, in contrast, would only have preferences to monitor cars/vehicles.

For instance, our survey results indicate that 33% of women and 29.5% of men agreed that one of the purposes for smart systems could be to monitor family members (see Figure 3).
Indeed, in the cyber domestic violence dimension, strangers are not the primary culprits but partners or family members often are the ones that initiate security breaches, look to enhance control and stalk partners (Refuge, 2018; Leitão, 2019). Observations on this matter were brought, respectively, by survey respondent F996 and focus group participant FGMF, as they expressed: “Sometimes couples use it to spy on each other” and “I don’t know if you watch Coronation Street... a gentleman and his partner have split up and he left a camera in her house, so he’s been watching her from his house, so that goes on.” Research in this area has explored how certain technologies could facilitate constant surveillance on partners through tactics such as digital monitoring and tracking to enable perpetrators varied forms of control (Dragiewicz et al., 2018; Harris and Woodlock, 2019). Simultaneously, these provide perpetrators with quicker access and methods to harass and abuse (Melander, 2010).

For Stark, stalking is “the most dramatic form of surveillance used in coercive control fall in a continuum with a range of surveillance tactics whose aim is to convey the abuser’s omnipotence and omnipresence (Stark, 2012; p 25)”. Therefore, digital technologies can provide the sense of being ever-present in the victim’s life. Fraser et al. corroborates that “one of the most terrifying tactics used by stalkers is to make the victim feel that she has no privacy, security, or safety and that the stalker knows and sees everything (Fraster et al., 2010; p 44)”. In this sense, although a victim might be separated from his/her partner, they have not been able to completely escape their presence in their lives (Dimond et al., 2011). Similar to these sensations, feelings about being observed, also emerged in both of our qualitative methods. For instance, FGLF stated “Who knows who is going to be listening to you or watching you. I would constantly feel unease knowing that someone is sitting in the back just watching me.” FGLM commented that “For me, when looking at surveillance, it’s like you’d say there are the good aspects and aspects where it could be open to abuse.” And M512 expressed: “It’s like Big Brother watching all the time. Potentially, very dangerous.”. In addition, participants in our focus groups mentioned how these technologies could facilitate being stalked. For example, FGMM said: “[Nest camera] You could use it when somebody doesn’t really know is been watched. I’m following you and you don’t know that I’m following you’ and FGMF: “Stalking is the only use I can see in Ring Cameras.”.

Certainly, within the smart technologies universe, each device could be used for monitoring purposes. For example, Interval House (2019) found common means to carry out stalking through technology. For instance, perpetrators could slip small tracking devices into their victim’s clothes or use smart security locks to either lock out or lock in their victims. Abusers could use location-based services (such as find my iPhone), parental tracking or other safety services (e.g. Find my Friends) to track their victims, which could result in potentially dangerous physical stalking (Freed et al., 2018). Other forms of stalking are facilitated by apps. For example, abusers could use the geolocation posts on Facebook, Instagram or Snapchat to track their victims’ activities and show up in person or let their victims know where they are (Woodlock, 2017).

For example, the Washington Post (2019) and Thebault (2019) reported that an Australian woman’s ex-boyfriend stalked her for months by using smartphone apps linked to her Land Rover. With this, the perpetrator was able to control her windows and stop the car remotely. Besides hacking connected devices, cyberstalking can also be conducted through the use of stalkerware and/or spywares. The use of such applications grew by 40% in 2019, according to 67,000 users having stalkerware apps installed on their phones in 2019 (Webb, 2020). Recurrent forms of monitoring and violence have victims report that they feel constantly unsafe as they cannot truly escape from their abusers, regardless of their physical location (Dimond et al., 2011). Indeed, results from the National Network to End Domestic Violence found that 50% of victim service providers report that offenders constantly use digital platforms and mobile apps to stalk victims and another 41% reported that abusers use GPS tracking devices (Young and Saxena, 2019). Based on this, the New York Times reported that centres for domestic violence have noted that abusers were monitoring victims’ activities or remotely controlling smart home appliances and smart systems. Whilst other victims report that they had their “thermostats kicked up to up to 100 degrees” or their “smart speakers turned on in the middle of the night (Bowles, 2018).”.

Certainly, participants in our survey noted that “smart systems are invading privacy and over-monitoring users” (M18) and that they are an “invasion of privacy as they are listening all the time” (F582). Another survey respondent felt uncomfortable around such technology: “I don’t like the idea of AI listening into my conversations.” (F995). Overall, 54.5% of male and 60.6% of female respondents agreed that smart systems could be intrusive (see Figure 4). Pertaining to one of our themes on domestic violence, features of digital communications such as storage, synchronicity, replicability and mobility (Baym, 2011) enhance abusers’ ability to persist intruding on their targets regardless of their location. In turn, perpetrators’ dimension of control goes beyond previous spatial boundaries and become more intrusive. According to FGLF, “smart systems are intrusive, it’s full of cameras or devices always watching you, microphones that are always listening to you.” The intrusiveness of smart devices was not only brought in our focus groups, but also, results from our survey indicate that users perceive these technologies as an invasion of their privacy. This view is illustrated in Figure 4, below.

Working from the premise that smart systems do not require face to face encounters and acts of violence can be perpetrated regardless of the user and perpetrator location, we argue that these devices could facilitate domestic violence to occur 24 h a day. Indeed, (Stark, 2012) identified that victims in this situation felt a condition of “unfreedom entrapment”, which key feature was to micro-regulate victims’ everyday behaviours in private and public spheres, restricting access to both (Stark, 2007; Woodlock, 2017). It is under this context where discussion of coercive control has emerged. For instance, (Stark, 2007) argues that coercive control is a theoretical framework that entails physical abuse that occurs not only within the settings of domestic violence but also includes tactics that are not traditionally considered as serious forms of abuse. To this, Reed et al.,

---

8Software that enables someone to monitor activities on another’s device without their consent.
add that digital technologies belong to a “constellation of tactics” within abusive relationships to allow the perpetrator to achieve certain goals, such as sexual gratification, coercion, retribution, humiliation, and exert control. Woodlock (2017) and Stark (2007), thus, concurred that although women can be abusive in intimate relationships, men often are the main perpetrators of coercive control, due, in part because it is a form of violence rooted in systemic inequality, which affords men a sex-based privilege (Woodlock, 2017). Given the rising number of coercive control offences (Stark, 2018; Stark and Hester, 2019) the UK has recently passed a Domestic Abuse Bill, which provides a new definition of domestic abuse and controlling and manipulative non-physical abuse. The Bill aims to enable everyone to understand what constitutes abuse and thus, encourage more victims to come forward (Home Office, 2019). In addition, the UK government has passed a legislation that positions coercive behaviour in an intimate or family relationship as part of a Serious Crime Act. The offence applies when: “A repeatedly or continuously engages in behaviour towards another person, B, that is controlling or coercive; and At time of the behaviour, A and B are personally connected (The Crown Prosecution Service 2017, Section 76, p.n/a).”.

### 4.3 Parental Control and Surveillance of Children

Figure 5 shows noticeable differences in smart systems attributes. For instance, men value privacy and comfort more than women. However, females were more concerned with aspects related to control, trust and the environment. Convenience, however, was almost equally rated. For this section, we note that surveillance occurs in many settings of our lives, in different relationships and zones, and is not confined to abusive relationships. For instance, Taylor and Rooney (2019), Hasinoff (2017) and Leaver (2017) discuss the role of digital technologies in parental surveillance (as we later present). Whilst others study the role of digital technologies in governmental surveillance (Marwick, 2012; Gallie et al., 2016; Han, 2017; Kendall Taylor et al., 2020; Mello and Wang, 2020), which may lead to denial of services and even destruction of property (Kleinrock, 2004). In sum for Zuboff, (2018) “nearly every product or service that begins with the word “smart.” or “personalised.”, every internet-enabled device, every “digital assistant.”, is a simply supply-chain interface for the unobstructed flow of behavioural data on its way to predicting our futures in a surveillance economy.”.

Tension in our survey and focus groups emerged when discussing using smart systems to monitor young children. As represented in detail in Figure 6, results from our survey indicate that only 29.8% of men and 31.7% of women agree to use these technologies with this end. However, most participants in our focus participants felt comfortable monitoring young children. To illustrate this point, FGMM said: “Baby monitors, when they’re sleeping. Definitely not a problem with that That would be the only camera I would have inside my house.” On this, FGLM expressed: “if you have children, you may want to be watching what they’re up to.” For some, invading baby’s privacy was not an issue, as elaborated by FGLM: “It’s a very helpful baby monitor. And if somebody wants to track the behaviour of my two-year-old grandson, they’re welcome to it.” Another FGLM stated that it was “completely acceptable to monitor a young child upstairs while you are downstairs.” and that “smart systems have great potential to stop kidnappers and alert the police or others about kidnapping from a remote location.” Indeed, we
will return to this point about smart systems possibly stopping abuse in Section 5.

Nonetheless, reasons to distrust technologies designed for children should be on parents’ radars given the 45 million online photos and videos of children been sexually abused and, in some cases, tortured. Keller and Dance (2019) found an insatiable criminal underworld that has exploited the flawed and insufficient efforts to contain these horrific imaginaries, given that criminals are using advanced technologies like encryption to stay ahead of the police. Similar experiences are noted by Chiu, (2019), who reported that through a Ring camera, an eight years old girl not only was subject to racial slurs, she was also told to break her television by a hacker—he continued pestering and harassing the little girl until the parents disconnected the device. On this, FGSF commented: “there are some horrible people out there absolutely vile people, they will definitely take advantage of some of these things”. FGLF added that “I want to trust smart systems more, I would love to trust them more. But I don’t.”

For Madden, (2016), regardless of users undergoing negative experiences, “smart” parental tracking is the logical result of a
world where children spend a significant part of their lives in the
digital arena. Nonetheless, over-monitoring children could lead
to negative outcomes, as shown by Hawk et al., (2009) when they
reveal that if parents engage in highly intrusive behaviours over
their children, it may backfire on them, as children may adopt
more secretive behaviours, thus, unhaling parents to know less
about their children’s activities and whereabouts. Given that the
technology of parental control has evolved so rapidly, there are
not yet clear norms of what is acceptable or even healthy in
demarcating monitoring boundaries (Weir, 2016).

Ironically, in some cases, children themselves ask for smart
systems that could be used to monitor them. Focus group
participant FGLM said:

It’s so I can keep in contact with my children. Our kids said we
needed them [smart systems]. Children’s schools they wanted to
have constant contact with parents and having a reliable way they
could be contacted.

FGSF noted that:

When you join school now, you’re generally expected to do
some element of your homework using Google or exploring
online. So, children are encouraged from an early age to use
digital technologies. Because if they do not, they are going to be
excluded from the world.

Parents observations on this matter were apt, given that the
UK government, through the Education Technology (EdTech)
program, seeks to tackle day-to-day challenges faced in the
education sector, including reducing teacher workload,
increasing efficiency, improving accessibility and inclusion and
improving teaching and students’ outcomes. The program seeks
to tackle these challenges by using tablets, laptops and/or other
digital devices (Department of Education, 2019). Demonstrating
how much the industry has grown so far, investments in EdTech
have reached £90.9 million—a 140% increase in the amount
invested in 2016 (Robins, 2019).

4.4 Femtech, Menstruation and Pregnancy

Another set of concerns arise through the monitoring of smart
systems related to menstruation and pregnancy. In our survey, as
Figure 7 illustrates, 28.9% of women and 20.3% of men agreed to
use these technologies for that purpose. Yet, people could have
reasons to distrust technologies accessing personal data to
monitor menstruation and pregnancy cycles.

Given the potential scenarios for misusing personal
information, focus group participant FGSM expressed being
distressed on where their data in general was going:

"For me, the biggest fear, it’s the data that they’re collecting that I don’t
know about. I think it’s the analytic data that they’re generating on you. They can tell what you like, what you
don’t like, they even can tell what your personality is."

These concerns were not far from reality, as many manufacturers of
smart devices base their primary business model on collecting
household data (Naughton, 2019). Not only that, Zuboff,
(2019) notes that consumers are unaware of the value of the
data they are giving away, which is not only extremely valuable
but also can be profitable to generate predictions about
preferences and future behaviours. Focus group participant
FGLM shared a similar perspective when he stated:

“The people who are benefiting now, and will do so more in the
future, are the people who own the data that’s generated by
smart technology, and then use that data to influence others’
behaviour”.

In this way, although participants seemed to be aware of some
of the instruments that regulate smart systems, many still did not
know what sort of personal information they were giving away
when accepting terms and conditions. To this, focus group participant FGMF stated: “all these are signed up to GDPR, aren’t they? but it concerns me that maybe there are hidden ways of, I’m not saying that there’s any subterfuge going on, but sometimes you might not have ticked a box, so that inherently gives them permission to use your data in certain ways. I find myself checking more carefully now.”. Indeed, most participants were unaware of what information users are giving away when agreeing to terms and conditions. Focus group participant FGMM concurred and asked in the room: “how many of us actually read all the documentation and terms and conditions?”. Certainly, most consumers are not reading them properly, for example, Amazon states that users have given permission for human verification and allows to use data “to train our speech recognition and natural understanding systems (Hern, 2019).”.  

Focus group participant FGLF explained in her experience why this could happen: “Basically, they designed the interface to make you just click through and ignore and just give them all they need.”. This vision could be accurate given that study conducted by McDonald and Cranor (2009) calculated that users would take up to 76 working days to read through all the privacy policies encountered in a year. In this sense, LifeHacker provides the internet users with the criteria for skimming through privacy policies. They advise users to look at statements related to data sharing, storage and collection or phrases such as “store’ and encrypt.”. Additionally, they advise users to search for terms such as “deletion” or “retention.” to learn about how long platforms keep their information (Grauer, 2019).  

5 DISCUSSION: SMART SOLUTIONS TO COMPLICATED PROBLEMS  

This section builds on our results to discuss three prominent qualitative themes: a duality of smart systems functions and emotions, the political economy of knowledge production, and the promise of smart systems for actually deterring and inhibiting abuse and violence.  

5.1 A Plurality of Functions, Beliefs, Attitudes, and Emotions  

Results from our study indicate that there are discrepancies in users’ beliefs and attitudes towards smart systems. For instance, although most participants knew about the risks these technologies entail and expressed being afraid of these concerns, participants still stated seeing the potential by which smart systems could ease their lives. We thus argue that the feelings and attitudes users have towards smart systems are complex, with a duality of positive and negative dimensions. Below we further elaborate on this thought.  

First, our data was not uniformly critical of smart systems. In some instances, smart surveillance fulfilled its purpose. For instance, survey respondent F898 avoided being robbed by monitoring his/her property: “Caught a burglar in my home on Canary camera but police still don’t have any one arrested as yet.” Monitoring has also helped to avoid food waste as noted by survey respondent M350: “As by-product, we noticed while on holiday our hive wasn’t active—we asked a family member to check, and there had been a power-cut which tripped the breakers. Saved us at least £300 in freezer food”. FGMF said that smart systems helped her to keep in touch with family: “I use technology for a range of applications but mainly to keep in touch with younger members of my family.”. Whereas survey respondent M703 perceived smart systems as a mean of enhancing relationships: “They can provide a way of aiding relationships”.  

Focus group participant (FGLM) captured a possible explanation of the duality of feelings, when he elaborated: “Despite my nightmare scenarios, I’m positive about it. It may seem really odd, but I am. I hope that we’re going to get the built in, we’re going to get to a point where we start to legislate more personally, and people are going to legislate for us, so we can get more control over these things.”. Or focus group participant FGMF, who regardless of discussing risks, still felt optimistic: “There are some reservations, which we’ve discussed, but I think it’s healthy to questions things and not just to accept them blindly, but yes, on the whole, I feel positive towards smart technolog.”. Another FGLM was even more explicit about the duality of smart systems, stating that "smart systems have a duality to them, they can turn into a ‘can do’ technology, they can become tailored to actually help those who have been disadvantage before, the old and frail, the victimized, tailored to their needs. They can become empowering.”  

Others discussed dual or at least mediated uses for their smart systems. FGLF stated that their approach to navigating the risks of smart systems was to use them when out of the home. As they said:  

Yes, I would use smart systems to monitor and survey my home. I am going to get a high view camera. Take it offline when I am home. I do not want it to surveil me, but I do want it to surveil intruders. But I don’t trust it enough to have it on all the time, so my solution is to unplug it when I am home.  

This suggests one possible way of managing smart systems to not overly force trade-offs over privacy or surveillance.  

5.2 The Political Economy of Smart Homes and Knowledge Cocreation  

Moreover, our findings indicate knowledge about smart homes has its political economy, it is distributed unevenly and sees some groups advantaged and other groups disadvantaged. Companies and providers may know very well about the parameters of smart homes, but many users and prospective adopters do not know what smart systems are. Hence, it is hard for users to identify how benefits are delivered and quantified and how risks affect their lives. On this matter, FGMF commented: "I think if there was a definition of smart technology it might help with understanding it better. Now it feels quite broad and vague.”. The fact that even within literature, there is a plurality of definitions and concepts of smart systems and to date, we do not have an accepted definition also makes it hard for policymakers to regulate them, not only in terms of privacy and data but also in terms of energy consumption and waste.
Finally, this lack of knowledge extends to manufacturers and authorities to advise victims of technology abuse. Where not only victims have had to deal with this situation on their own, but also demands immediate action to enhance their regulatory framework. Beyond technology abuse, industries’ lack of expertise has also led users to feel these technologies are hard to fix and thus leading to over consumerism and disposable culture. Supporting this sentiment, FGLM commented: “Most of the items are designed to discourage you from repairing them, and most of the perceived wisdom is that you can’t repair them, or you’re told culturally that you’re not to repair it”. FGLM concurred: “The built-in obsolescence of all the smart technology we are purchasing some apps after a year will no longer update”.

5.3 The Promise of Smart Systems Inhibiting Violence and Abuse

In other cases, smart systems have helped prevent domestic violence. Indeed, there are an increasing number of personal safety apps that are designed to make users feel safer, in particular for women (Maxwell et al., 2020) whilst other technologies target children’s safety (Hasinoff, 2017). For example, in New Mexico a man was arrested for beating his girlfriend and threatening to kill her. During the assault, he asked: “did you call the sheriffs?.” The question was picked up by Amazon Alexa and recognized as a command, prompting to call 911 (Miller, 2017). In addition, many smart speakers have unobtrusive recording features that could provide evidence of abuse. Other app-based bottoms or Bluetooth trackers can allow victims to send silent messages calling for help or record dangerous situations.

In order to prevent domestic violence, Brignone and Edleson (2019) review the quality and potential use of smartphone apps to intervene in intimate partner violence either in domestic settings or through an app. This study takes upon more relevance when research has shown that meeting online had finally overtaken meeting through friends, with around 40% of US couples first connecting through an app (Kjellson, 2016). Their work (Brignone and Edleson, 2019), found that higher rating apps such as Tech Safety, Over the Line and Youth Pages often had accessible user interface, updated and functional links to keep victims informed. In addition, such apps possessed technical capabilities that were mindful to the victim’s safety, such as turning off location tracking and the safe and secure storage of user data and developers. After an exhaustive review, Maxwell et al., (2020) found a common trend within the safety apps world, where the majority offered interventions either at the time of the event or post-event. Their results suggest that they may reduce a user’s fear of crime; however, such applications have limited usefulness in reducing vulnerability to victimization (Maxwell et al., 2020)

A similar approach is taken by Freed et al., (2017) They refer to the works of (Arief et al., 2014) and (Emms et al., 2012) to better design platforms to help victims. The first lays out a vision for ‘sensible privacy’. Their app would erase information about visits to victims-relevant websites by a user and record potential abuse associated with the device. The second suggests tools to help victims of domestic violence erase their browsing history. Other digital platforms, such as GuardDV, (2019), aim to protect victims of domestic violence with real-time information about the safety of their environments through the use of smart monitoring and facial recognition technology. Other apps for victims of domestic violence have been developed, including BrightSky developed by Vodafone and Hestia (Vodafone, 2019) TechSafety app (Safe Chat Silicon Valley, 2019) and others. Given the constant pressure from users to protect them, Tinder released some new safety features such as a panic button that alerts authorities and a photo verification feature. However, research indicates that these measures are inadequate it puts the onus on women, rather than the app itself and Tinder’s poor reaction to act and suspend users with aggressive behaviours.

The prevention of domestic violence is not limited to smart systems apps. Ogilvy, for instance, is developing an e-textile technology that keeps a record of events. The smart clothing device is known as ‘The Dress for Respect’, and for some, it will bring sexual harassment into the limelight. These dresses have sensors sewn into them that record contact and pressure. In this sense, when contact happens, the same area lights up on the dress on the control unit’s computer screen. This technology can also keep track of events (e.g. time and location) and even notes the intensity of the touch, as the sensors record the presence of touch and pressure (Murphy, 2018).

Governments provide other security measures. For instance, the Australian Office of the ESafety Commissioner, (2019) provides useful advice to users on what to look out for when purchasing smart devices. The guide’s contents explain how to be safe when using these technologies in a clear and friendly format in addition to age recommendations. Alternatively, the FBI, recently warned users about features that come with enhanced televisions and guard questionable data collection, could be used for monitoring purposes and as a gateway for hackers to come into users’ homes. The FBI warns about the range of threats smart devices could entail, from changing channels and showing children inappropriate content, to turning the bedroom TV’s camera and microphone and silently cyberstalk users (FBI, 2019).

However, although efforts from the government are made to address cyber abuse, others suggest that to address domestic violence is necessary, first, that victims understand the nature of shared devices ecosystems; whilst manufacturers ought to be more transparent in terms of who access users’ accounts (Parkin et al., 2019). Whilst Webb (2020) is more determine when she suggests that “Stalkerware shouldn’t exist at all, because it’s unethical.”. A middle point is suggested by researchers indicating that a feminist approach should be developed considering values and views from domestic violence victims that embed their views, values and experiences in the apps design and innovation (MIT Technology Review, 2020). On this point we note that to further mitigate technology facilitated abuse, victims should contribute and actively participate in the development of technologies and apps that prevent abuse. Like Diaz-Gorinkiel et al. (2021) we argue that technologies alone do not represent a permanent solution to the problem of domestic
technology and our online environment may make it conventional forms of abuse, the ubiquity of digital data manipulation and intrusiveness. Moreover, unlike children—especially women and girls—tracking, control, and abuse people independent of the victim or perpetrator with smart systems making possible abuse 24 h of the day of the week. The smart systems dimension, where devices are tools of surveillance, control, and domestic and sexual violence in households and pregnancy in some circumstances. Under this context, we see domestic violence as well as companies opening up vulnerabilities to hackers and third parties with the perpetrator of abuse a family member or relative), but also members. Many discussed monitoring children, a concern not purposes for smart systems should be to monitor family members. Our results reveal some interesting findings concerning the acceptability of surveillance and monitoring. Almost one-third of all survey respondents, or 33% of women and 29.5% of men when broken down by gender, agreed that one of the purposes for smart systems should be to monitor family members. Many discussed monitoring children, a concern not only if those parents abuse their children (the most often perpetrator of abuse is a family member or relative), but also opening up vulnerabilities to hackers and third parties with the remote access that can facilitate cyber stalking. Contrary to the glossy and optimistic accountings of smart systems in its promotional material, our findings suggest that users of smart systems although they did not vividly state been victims of technology abuse, they recognized their dark side and dystopic ends; including their potential to exacerbate domestic domestic violence as well as companies “sinister” means for data manipulation and intrusiveness. Moreover, unlike conventional forms of abuse, the ubiquity of digital technology and our online environment may make it difficult to ever truly escape such abuse once it begins, with smart systems making possible abuse 24 h of the day and independent of the victim or perpetrator’s physical location. It may create future hostile digital environments that track, control, and abuse people—especially women and children—from the earliest stages of their life, from conception and pregnancy in some circumstances. Under this context, we make an imperative call to further advance the understanding of surveillance, control, and domestic and sexual violence in the smart systems dimension, where devices are tools of entertainment and security and instruments of harassment, coercion, and abuse. We also call on those designing smart home and prosuming systems, especially analytical protocols and software algorithms, to be more aware about cultural sensitivity and gender issues (Sovacool and Griffiths, 2020) as well as data sensitivity and algorithmic justice (Rahwan et al., 2019; Panetta, 2021)

Nonetheless, our findings were not entirely negative. Like many tools, smart systems possess a duality to them, there are configurations and options where they can prevent and inhibit abuse, via smart clothing that automatically detects a physical assault, to cameras or systems that offer real time assistance to the police for catching criminals and documenting abuse, to apps and devices that help the victim recover from abuse, too. Which pathways smart systems proceed down will depend greatly on how the technology is governed in the near future shaping its evolution.

Furthermore, given that women are not only victims of domestic violence, for instance, recent research has indicated that women are just as likely, if not more so, to engage in more covert forms of stalking such as cyberstalking (Berry and Bainbridge, 2017; Smoker and March 2017). Moreover, the works from Hine et al. (2020), Perryman and Appleton (2016) and Lysova et al. (2020) identify women as the perpetrators of domestic violence we encourage future research to look at other groups of domestic violence and further analyse what the role of technology abuse is in gay couples, for instance. Lastly, our work points the way towards fruitful future research. Although the dominant lens we utilized to view our results was grounded in domestic violence, feminist, especially energy feminism, offers a notable alternative framework for other researchers to pursue. For instance, Bell et al. (2020) suggest that themes of feminist political control over energy systems, systems that prioritize welfare or the environment over profit, efforts to mitigate violence and promote a culture of care, and efforts to promote community-directed and collaborative energy systems would yield deeper insights than a “gender only” lens.

Furthermore, we call on researchers to consider more intersectional forms of gender and energy or smart technology that go beyond many of the simple binaries implicit within current research, e.g. gender (male and female), income (rich and poor), or race (black and white) (Crenshaw, 1991). Ground-breaking work in this regard focusing on technology includes that of Mulvaney (2013) (examining justice and solar commodity chains), Adams et al. (2012) (examining justice and whole systems analysis of microgeneration technologies), and Healey et al., 2019 (embodied energy injustices). Ground-breaking work approaching it from the intersectional angle includes Lennon (2017) (intersections of race, ethnicity, and gender), Ryder (2018) (intersections of feminism, class, and power), and Lieu et al. (2020) (intersections of indigenousness and gender). Perhaps when these more integrated, reflexive, and intersectional approaches are utilized, we can better understand and begin to resist the forms of patriarchy and violence that are at risk of being embedded into the smart energy systems, grids and prosuming practices within the homes of tomorrow.
AUTHOR CONTRIBUTIONS

All authors listed have made a substantial, direct, and intellectual contribution to the work and approved it for publication.

FUNDING

The authors gratefully acknowledge support from UK Research and Innovation through the Centre for Research into Energy Demand Solutions grant reference number EP/R035288/1.

REFERENCES


ACKNOWLEDGMENTS

Donal Brown from the University of Leeds, Matthew Lipson from the Energy Systems Catapult, and Ben Walker, Harry Bradwell, and Joshua Phillips from the Department for Business, Energy & Industrial Strategy in the United Kingdom all offered very helpful suggestions on the survey design utilized in this study. We also benefitted substantially from earlier work on smart homes from Charlie Wilson and Tom Hargreaves at the University of East Anglia, who shared with us their survey instrument and offered additional suggestions on design.


Conflict of Interest: The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher’s Note: All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

Copyright © 2021 Sovacool, Forszyfer-Del Rio and Martiskainen. This is an open-access article distributed under the terms of the Creative Commons Attribution License (CC BY). The use, distribution or reproduction in other forums is permitted, provided the original author(s) and the copyright owner(s) are credited and that the original publication in this journal is cited, in accordance with accepted academic practice. No use, distribution or reproduction is permitted which does not comply with these terms.