MAKING IOT SECURITY POLICIES RELEVANT, INCLUSIVE AND PRACTICAL FOR PEOPLE: A MULTI-DIMENSIONAL METHOD

Kruakae Pothong[1], Larissa Pschetz[2], Jeremy Watson CBE FREng[3], James Gbadamosi[4], Andre Asaturyan[5]*

[1] *Dept. Science, Technology, Engineering & Public Policy, University College London, London, UK*
[2]*School of Design, University of Edinburgh, 47 Potterrow, Edinburgh, EH8 8BT, UK*
[3]*Dept. Science, Technology, Engineering & Public Policy, University College London, Euston House (8th Floor) 24 Eversholt Street, London, NW1 1BS, UK*
[4,5]*Smart Homes & Buildings, Building Research Establishment (BRE), Bucknalls Lane, Watford, Hertfordshire, WD25 9XX, UK*
**k.pothong@ucl.ac.uk*

Keywords: IoT security, deliberation, design, simulation.

Abstract

Growing amounts of research on IoT and its implications for security, privacy, economy and society has been carried out to inform policies and design. However, ordinary people who are citizens and users of these emerging technologies have rarely been involved in the processes that inform these policies, governance mechanisms and design due to the institutionalised processes that prioritise objective knowledge over subjective ones. People's subjective experiences are often discarded. This priority is likely to further widen the gap between people, technology policies and design as technologies advance towards delegated human agencies, which decreases human interfaces in technology-mediated relationships with objects, systems, services, trade and other (often) unknown third-party beneficiaries. Such a disconnection can have serious implications for policy implementation, especially when it involves human limitations. To address this disconnection, we argue that a space for people to meaningfully contribute their subjective knowledge – experience- to complex technology policies that, in turn, shape their experience and well-being needs to be constructed. To this end, our paper contributes the design and pilot implementation of a method to reconnect and involve people in IoT security policymaking and development.

1 Introduction

The added abilities of physical objects to sense, actuate, collect and process data, as well as communicate with other physical objects, systems and humans offer great opportunities. However, these so-called smart, connected features that characterise the Internet of Things (IoT) also increase the risk of attack. With a compound annual growth rate of 33% since 2013, bringing the global number of IoT devices (cellular connected devices) to 4.1 billion in 2024 [1], the attack vectors are spiralling. 60% of these IoT devices are consumer devices [2]. Yet, few consumers adequately understand how IoT devices operate, or can keep track of the vulnerabilities of these devices and their consequences. Consumers and citizens have not been adequately involved in the development of policies and design that shape IoT security and the way the technologies work.

In addition, many people have a poor sense of efficacy when it comes to influencing the way technologies work, as they are often cast as recipients, rather than partners in relevant development processes. There is a perception that the general public does not have the knowledge needed for institutionalised policymaking. This perceived knowledge gap is only going to widen as technologies advance toward increasing human-delegated agency and mediate people's relationships with objects, systems, services, trade and other (often) elusive third-party beneficiaries. This reinforces the disconnection between people and the policymaking processes and can have serious implications for policy implementation. We argue that this gap needs to be bridged. Thus, we contribute a method to reconnect people with technology policy development to help policymakers and relevant actors develop IoT security measures that are better aligned with people's value preferences.

1.1 Scope and objective of the paper

This paper provides snapshots of an IoT attack landscape and the policymaking traditions in democratic jurisdictions shaping the development of IoT security and design. These snapshots identify IoT security as a 'wicked' problem, justifying the requirement for increased public participation in the dynamic policymaking and design to tackle it. The attack landscape also guides our development of simulation for the pervasive IoT deployment in the home and the plausible attack scenarios. The paper details the design and pilot implementation of our approach to engage the public in policymaking, design and development processes concerning IoT security.

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.

1.2 Methods and Foundation

This paper takes a multidisciplinary approach in developing a method of inquiry and constructing a space for public participation in policy and development concerning IoT security:

- *The computer science element* simulates the pervasive deployment of IoT in a domestic environment in a controlled (intended) condition as well as in scenarios where IoT devices are compromised on various scales.
- *The arts and humanities element* organises human experience in the scenarios and speculative design, represented by futuristic prototypes of autonomous devices.
- *The social science element* uses deliberative exercises to capture human reactions to and reflections on their experience, as well as observing how people's values and preferences shift after been exposed to particular experiences and ideas.

As part of PETRAS IoT in the Home Demonstrator, members of the public in London and Hertfordshire were invited to participate in our simulated deliberative events. These were held at the Building Research Establishment (BRE) on 19 and 20 January 2019. A total of 17 people of diverse demographic backgrounds and technical skills participated in this pilot research. To evaluate this approach pre- and post-session surveys were conducted to observe whether and how people's sense of efficacy (perceived ability to influence changes) would be affected by participation.

2 IoT security – a wicked problem

Reports of exploitation of vulnerabilities of smart, connected devices and digital technologies are increasing in frequency, adversity scale, diversity of targets and types of attacks. Cisco has reported the evolution of self-propagating malware, such as Nyetya-wiper, masquerading as ransomware, the advancement in the use of encryption, cloud services and other technologies used for legitimate purposes to disguise malicious command-and-control (C2) activities, and increasing exploitation of security gaps in the rapid growth of IoT and use of cloud services [3]. The consequences of such exploitation vary in scope and scale. They have implications for physical functionalities and incur unnecessary costs, but also affect the safety, security and privacy of individuals as well as the stability and security of the nation.

Research shows that popular domestic smart connected devices, such as cameras, motion sensors, smoke alarms, light bulbs (Philips Hue), power switches, talking dolls, controller (Samsung SmartThings), voice assistant (Amazon Echo), Smart TV with Google Chromecast and speaker, all have vulnerabilities in integrity, access control or reflection capabilities [4]. These vulnerabilities can be exploited to facilitate the 'man-in the-middle' attack, denial of service attack (shutting down devices such as a smart smoke alarm), a password-guessing attack and attacks through Domain Name System (DNS) protocol, stalking and harassment. Consequences of these attacks range from financial losses to compromised physical and mental well-being.

Connected devices have been recruited as botnets in a larger scale of denial of service (DoS) attacks – a new family of DoS bots called *Chalubo* has recently been reported [5][6]. Attackers can target businesses' IoT enabled manufacturing and supply-chain, as observed in the case of *Dragonfly* and *watering hole attacks* [7]. Exploitation of IoT vulnerabilities can bring a country to its knees, as seen in the continuous cyber-attacks on state and private infrastructure in Ukraine, including the Chernobyl nuclear power plant monitoring system [8].

The IoT security challenges have two interdependent dimensions – technical and social. The physical limitations of the computational and memory resources of IoT devices constrain their abilities to maintain confidentiality and integrity of IoT systems [9]. The communication between nodes, carried out across low-bandwidth channels, makes it difficult to design secure and robust systems [10]. The heterogeneity and the number of interacting devices and components in IoT systems render it virtually impossible to develop and implement adequate security solutions. The social dimension is seen in the varying skills, knowledge and awareness of security among people who interact with IoT technologies in various capacities (e.g. consumers, industrial system operators, etc.), which makes maintaining IoT security even more difficult and unpredictable.

The evolutionary and adaptive nature of the technologies, as well as the scope and scale of their consequences, mean IoT security is categorised as a 'wicked problem' [11][12][13]. It is 'wicked' because it is complex, involving interdependencies between physical and social sciences, fast-changing patterns, difficult to predict and diverse value preferences. Addressing this 'wicked problem' of IoT security, this paper argues, in line with other critics [14][15], that the rational-technical approach that dominates governance of sciences and technologies is inadequate. Technologies themselves are fast-changing; the actual usage and consequences of mass adoption are often unpredictable; so are the results of any policy intervention. Moreover, the rational-technical approach often prioritises the risk-benefit calculation, objective evidence, to the exclusion of subjective evidence/experience. Yet, individuals' experience both constitutes and is constituted by their value preferences and contributes to the 'wickedness' of the IoT security issue and broader social problems.

3 Public policy (dis)engagement

From the political perspective, the rational-technical approach in developed democracies such as the USA, EU

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.

(European Union) and UK tends to concentrate decision-making power among the well-resourced few. Here, the relevant resource is knowledge. This implies a relationship between knowledge and power.

In the USA, the emphasis on small government, limited governmental power to create and maintain social order and a legal requirement under the Administrative Procedures Act (APA) have resulted in reliance on expert knowledge and facts to legitimise government intervention [16] and demonstrate impartiality [17]. Despite the American constitutional protections surrounding free speech and the right to assembly which allow for public opinion to shape government decisions and actions [18], policymakers have legal obligations to make decisions based on impartial facts. The reliance on value-neutral knowledge in the EU legislative processes resulted from the requirements under the Amsterdam Treaty that any decisions that result in legislation be based on research findings and facts [19]. Member states are required by the European Communities Act 1972 to transpose EU legislation into national law so this also affects the national level.

The UK is bound by the European Communities Act 1972, and even after Brexit, as long as the UK continues to trade with the EU, provision of digital products and services still has to comply with the EU regulations, such as General Data Protection Regulation (GDPR), the proposed Cybersecurity Act and the directive on security of network and information systems (the NIS Directive). The British version of representative democracy is characterised by 'a limited liberal conception of representation, a conservative notion of responsibility' [20] and the attitude of 'government knows best' [21]. Knowledge, in this case, is tied to the executive. Public consultations are often an empty formality aiming to impart a sense of involvement and people's consent to be governed [22].

The reliance on objective expert knowledge and limited public participation in policymaking across these democratic jurisdictions result in political disengagement and a poor sense of efficacy among people. It deters the public from contributing to solutions in matters that affect them. In the UK, there is a public perception that 'government is remote' [23]. The 2018 audit report of political engagement in Britain [24] showed that people's satisfaction with the government system and their sense of efficacy (the perception of being able to bring about political change) have been persistently low since 2004 and is getting worse, dropping to 29% and 34% respectively.

Complementing these findings are the results from the pre-deliberative survey conducted by the lead author on people's responses to pervasive IoT deployment in the home. It indicates that an overwhelming majority of research participants (83%) think that they have very little to no say at all on how smart connected technologies work, and 65% demanded more say over how these technologies work. Here, people's 'say' includes the perceived efficacy of their inputs into policies, regulations and design that shape it.

Given the political traditions, practices and complexity of IoT, technology users and citizens are at even greater risk of being excluded from the design of technology policies. However, people are one of the key contributing factors to the 'wickedness' of IoT security and they feel the socio-technical impact of IoT technologies. To tackle the 'wickedness' of IoT security, it is therefore important to include people in the design, development and policymaking processes.

4 Re-engaging the public in IoT security policymaking and design

We argue in line with critical policy analysts [25] and public management researchers [13] that responses to persistent and intractable problems require greater understanding and accommodation of diverse perspectives and interests. To achieve this, many have suggested a participatory approach, with an emphasis on the discursive element of policymaking processes [14][26][27][28] and the authenticity of dialogues [29]. Such emphases can bring out the value preferences of various stakeholders, providing insights into the framing of problems and the subsequent responses.

Building on this approach, we argue that future dialogues concerning the wickedness of IoT security should be re-centred on ordinary people who have often been excluded from direct participation in policymaking. Their experience with technologies should be brought to bear in the resolution of the 'wicked problem'. To re-engage people in these dialogues, we created a space and developed mechanisms for encouraging people to contribute their form of knowledge – experience and capabilities – in collective problem definition and resolution, concerning smart connected features of IoT. An immersive experience was constructed at the functional, sensational and rational levels, using simulated scenarios and speculative design. This immersive experience prompts people to share their perspectives and reflect on the immersive experience, thinking through what is problematic and how, given their capabilities, to best deal with this.

4.1 Simulated scenarios

Here, we use simulated scenarios to organise a common experience, following the arts and humanities tradition. These scenarios were designed to draw out people's feelings about their experience, and stimulate them to express their subjective accounts and reflect on them. These subjective accounts 'provide the material out of which social meaning is created' (p. 13) [30]. They help participants construct meaning from their previous dealings with technologies, their immediate insolvent and the organised experience in the IoT home. In addition, they 'often are the source of the propositions of arguments and frequently provide evidence of claims' (p. 13) [30]. More importantly, they 'help people to fit their bit of knowledge, experience or expertise into the larger jigsaw of policy debate' (p. 104) [31].

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.

The use of scenarios as a stimulus, here, follows the research tradition of using vignettes to draw out reflective responses from research participants. Vignettes serve as tools for extending discussions of issues underlying the scenarios and for collecting 'situated data' concerning collective values, beliefs, norms and behaviours [32]. Vignettes are used in research across various topics, including domestic violence and abuse [33], experience of physical exercise [34], end-of-life care [35] and risks [36].

In this paper, the scenarios simulated the known vulnerabilities of IoT in ways that trigger people to articulate their feelings and rationality about the benefits and consequences of pervasive IoT deployment, in both intended and unintended circumstances. We situated this pervasive IoT deployment within the home environment. The scenarios also translated findings from existing computer sciences research concerning IoT vulnerabilities into functionalities and incidents that people are likely to experience, physically and emotionally, should they welcome this set of technologies into their homes.

Advancing the work of Coleman et al. [37] and Pschetz et al. [38], the lead author designed the scenarios to be interactive. Research participants were invited to interact with the featured domestic IoT devices as though these were the devices in their own home. Volunteer research participants were invited to play the role of malicious agents, exploiting the known vulnerabilities of IoT devices and systems in the home while the rest were asked to play the role of household occupants. The interactive element of the scenarios provided room for participants to construct their subjective accounts of the underlying issues, consequences of IoT vulnerabilities, what any of these mean to the participants and how to respond.

The scenarios were divided into two key categories – intended and unintended functionalities/usage – to ensure a balanced view concerning IoT deployment in the home, highlighting that technologies can have both advantages and disadvantages. In the intended functionalities and usage, participants were invited to interact with active IoT devices and observe various data activities. Some of these devices included a version of a distributed energy system, embodied in the form of an energy-trading kettle, Philips Hue light bulbs, and Alexa assistant which served as a central control over the constellation of IoT devices in the home. Examples of the data activities included the live drawing of a floor plan generated by iRobot Roomba vacuum cleaner, a household energy consumption report and data generated by Philips Hue light bulbs.

The unintended usage featured scenarios of:

- a smart lock, which is connected to a voice control home assistant, being compromised, allowing a burglar to enter the participants' home and steal their valuables;
- Alexa assistant ordering a holiday package and charging the amount due to the participants' account, without command or agreement from the account owner;
- the dubious self-activation of the distributed energy trading kettle – nicknamed Karma Kettle.

4.2 Engineering simulation

The scenarios, particularly those concerning cybersecurity, used in this research were designed to represent the complex interdependencies and relationships between the different IoT systems and the ordinary people who have fitted out their homes with them. The engineering of these scenarios centred on three key elements: simulation, design and ordinary people. Simulation has been gaining in popularity as an approach for testing and assessing cybersecurity risks. However, existing cybersecurity research [39][40][41] often focuses on modelling interaction between attackers and the network of information systems, involving Edge devices (e.g. workstations, printers, connected lightbulbs), routers, applications, servers and databases. The core purpose of simulation in this context is to assess security risks in particular IoT ecosystems, which often under-represents the broader social and cognitive dimension of others involved (e.g. system administrator, users and security agencies) [42].

Few cybersecurity simulation scenarios capture both the technical and social dynamic of attacks. These include the Cyber ShockWave project [43] and the work of Gallaher [44]. The Cyber ShockWave project situated its cybersecurity simulation scenarios in the government's response to a large-scale national cyber crisis. Gallaher's scenarios were contextualised in the commercial provision of utility services. Neither captured cybersecurity incidents in domestic life and how ordinary people respond.

To fill this gap in research, we simulated scenarios featuring the social-technical dynamics of cybersecurity incidents in people's homes. The purpose of these scenarios was to simulate known IoT vulnerabilities, thus creating a common experience for ordinary people who have already started using or plan to use domestic IoT devices, rather than testing or assessing IoT security risks. The simulated scenarios served as a bridge for research participants to draw on their experience, knowledge and skills to reflect on this organised common experience, collectively define their problems and develop relevant responses.

In engineering the simulation, the fourth (Gbadamosi) and fifth authors (Asaturyan) explored vulnerabilities of a selected range of domestic IoT devices, including devices in the Amazon Alexa family, TP-Link HS100 and HS110 Smart Plugs, iRobot Roomba, Smappee Energy MonitorNest Camera and Philips Hue lights. Their experiment showed that attacks on these devices do not always require sophisticated technical expertise or valid credentials. They found that devices in the Alexa family, which currently do not use any form of voice recognition by default, can be exploited or unintentionally activated. This was observed in the case of a television advertisement being used to activate an Alexa Skill to order Purina cat food.

Vulnerabilities were found in the password rules of iRobot Roomba and Philips Hue Hub. The randomly generated passwords locked behind physical interaction with these devices would authorise access to most of the stored data and

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.

allow control. However, giving any passwords that match the length of a normal password and do not break any of the other passwords would allow access to most of the same data that a valid password would allow. The authors also found vulnerability through network connectivity of IoT devices such as the TP-Link HS100 and HS110 Smart Plugs. Access to the same LAN as these devices would allow complete access to these devices without any credentials, making them only as secure as the network itself. The connectivity of IoT devices can also be exploited through the abuse of the publicly available methods of device interaction detailed in the Application Programming Interface (API) or device technical specifications.

Based on these known vulnerabilities, the fourth and fifth authors simulated the social-facing cybersecurity scenarios in the home. In the intended functionality of a fully fitted IoT home, they used a Raspberry Pi to host all the code, written in Python and JavaScript, to generate the Graphical User Interface (GUI) for display. This enabled visualisation of energy consumption in the household, relevant costs and other data generated by the devices such as the live feed of the positions of the iRobot Roomba, which was then converted into a detailed floor plan and stored in the device history, accessible through the device application. Using Philips Hue Representational State Transfer (REST) API, the authors were able to visualise a huge volume of data accumulated by the device for participants. The accumulated data revealed occupancy patterns and the devices controlling the lights. The visualisation of the volume and types of data prompted research participants to think about their habits of use, the data generated, what can be deduced from the data, the consequences of such deduction and what any of this might mean for them.

In the unintended use of domestic IoT, the first and second scenarios both represent the exploitation of the absence of default voice recognition of home assistant devices in Amazon Alexa family. After the implementation of this scenario, the BBC reported similar incidents of a connected home assistance being exploited to control connected devices such as smart locks and smart cameras [45]. This report confirmed the plausibility of both scenarios, featuring the unauthorised access to control smart locks, smart cameras and other purchases by exploiting the vulnerabilities in the home assistant devices. The third scenario, featuring the dubious self-activation of the Karma Kettle, represented the difficulties for domestic users in determining whether such self-activation resulted from automated energy release from the grid or from malicious tampering. The possibility of malicious tampering was considered as a result of identified security vulnerabilities in the TP-Link HS100 and HS-100 Smart Plugs.

4.3 Speculative design

An artefact, nicknamed a Karma Kettle, was developed and used in both our intended and unintended scenarios to give research participants the experience of interacting with a more complex form of IoT technologies, connecting devices in the home to a broader constellation of systems and devices. The Karma Kettle represents the complexity, invisibility and opacity of the operation and connection of domestic IoT devices, user energy consumption behaviour, the energy consumption and management at a district or national levels, in distributed energy systems. The use of the artefact follows the tradition of speculative and critical design.

For this paper, the second author (Pschetz) designed the Karma Kettle, a speculative prototype, to stimulate discussions concerning the future of energy, taking into account the expansion of renewables, distributed energy systems and the evolving management of energy networks. The kettle fitted the context of smart, connected households and drew attention to the networked dimension of energy demand-supply management which is often obscured by the habits of electrical appliance usage. Distributed energy systems demand lower initial investment, thus allowing smaller enterprises to produce and sell energy, a sharp contrast to the traditional centralised national grids. However, distributed energy systems are burdened with issues concerning security – at both physical and logical layers – data protection, management and privacy. Moreover, embedded in them are degrees of autonomy for domestic energy users (who can also be energy suppliers) to mediate transactions, balance energy availability and pricing. This new capability raises questions of ownership, control and transparency: who defines algorithms that support autonomy, for whose benefit and how to explain the algorithmic operations to domestic users?

The Karma Kettle simulates the experience of interacting with a device that can store and trade energy according to fluctuations in energy availability and pricing. In this context, domestic batteries store part of the energy available in the grid, ultimately helping to balance on- and off-peak times and prices. Most importantly, the kettle gives participants degrees of control over energy transactions in a bottom-up, peer-to-peer manner. It displays states of scarcity and abundance of energy in the grid and in storage, and lets users decide what to do in this context. Participants operate the kettle through a rotary switch that allows them to use (boil), pull (store) or push (sell) energy, and give or deduct points from users for pulling and pushing energy into the grid according to the way this behaviour affects the grid in positive or negative ways. This contributes to participants' energy 'karma'. For example, if energy is highly available in the grid and in storage, users are encouraged to use it (they receive points for storing and using energy and lose them for pushing stored energy into the grid), contributing to a positive karma. If energy is scarce in the grid and in storage, users are encouraged to push stored energy into the network – using energy in this case would contribute to a negative karma.

While speculative design is broadly concerned with depicting what technology, society and the world could be, the Karma Kettle align with a more critical design approach. Critical design was defined by Dunne and Raby as a sort of 'design that asks carefully crafted questions and makes us think' – a contrast to affirmative design which identifies with commercial practices and emphasises 'solving problems and findings answers' [46]. Its aim is to use design to create artefacts that embody critical issues and provoke emotional responses, to help figure out what the world could be like. Critical design thus creates open-ended scenarios, providing artistic encounters with the functional aspect of human

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.

experience. The resulting emotional responses, particularly the negative ones, convey a sense of problems authentically conceived by those exposed to the experience, rather than problems formally defined and framed by others (e.g. researchers and experts) and given to people to solve. Officially defined or framed problems are known to undermine meaningful public participation in policymaking and design [47].

Ultimately, the kettle was included in the scenarios to motivate affective responses and reflection on the impacts of individual behaviours on the networked energy systems, the level and aspects of control individuals prefer to retain or delegate to associated entities in the distributed energy systems. The kettle was also featured in the unintended scenarios, when it suspiciously turned itself on and off. This suspicious behaviour of the kettle represented the blurred boundaries of the autonomy of domestic users, the connected and autonomous functionality of the device and malicious tampering on various scales.

4.4 Deliberation

Deliberation emerged as an alternative to expert-based public decision-making and in line with the growing number of stakeholders with competing interests, constituting greater complexity and uncertainty for policymaking. Theorists describe deliberation as a talk-based process for achieving mutually acceptable responses to social problems through exchanges of reflections on diverse perspectives, experiences, argumentation and persuasion [48][49]. Its principles of equal, open and reflective exchanges make deliberation accommodating of diverse views, interests, value propositions and power relations. Schön and Rein [50] named deliberation as a requirement for taming a ‘wicked problem’ due to its ‘recognition of perspectives and values that “frame” the definition of problems’.

Practices of public deliberation have been widely explored in the social sciences [49] [50] [51]. Deliberation has successfully been applied to critical design in the context of autonomous distributed energy systems [38]. However, deliberation had not been used in cybersecurity simulation to enable ordinary people to contribute their form of knowledge – their subjective accounts – to emerging IoT security policies and design. In this paper, deliberation is applied in four steps to connect participants’ sensations and the rational dimensions of their immersive experience, enabling them to collectively define problems and work out how to respond to them:

- Storytelling: an exchange of experiences related to the issues underpinning the scenarios;
- Problem definition: a scoping exercise, in search of problem definitions, taking into account diverse value preferences, interests, responsibilities and accountability;
- Solution brainstorming: a hatching of ideas for solutions and debating their merits;
- Resolution: a collective decision-making, shortlisting the meaningful recommendations for the problems identified.

This four-step deliberative process is adapted from the work of Coleman et al. [37]. This simulated deliberation allows researchers to observe how participants’ value preferences, interests and propositions change as they are exposed to new experiences, ideas and perhaps more convincing arguments. The analysis of this process provides a narrative about the IoT security that people anticipate, starting from the devices in their homes. In this way, people are involved in the construction of the narrative about IoT security that is meaningful to the sample participating in this research. Given the well-rounded human experience on which it is built, this narrative should, in principle, be meaningful to those exposed to similar experiences. This potential for greater public support for the resulting narrative on IoT security gives it legitimacy to guide the responses to the ‘wickedness’ of IoT security in policies and design.

5 Debating technology failure: Learning and insights

In our study, we carried out two pilot simulated deliberative sessions, with a mixed demographic of 11 and 6 participants, with diverse technical skills, interests in and expectations of IoT technologies. Our deliberation opened with the simulation of a scenario in which the IoT devices and systems fitted in their assumed home functioned as intended. In this scenario, participants were interacting with a range of utility IoT devices available in the market, such as Alexa Echo, which acts as a central control for the IoT home, Philip Hue light bulbs and iRobot Roomba. The initial reaction was a mix of marvel and scepticism. Participants were also invited to interact with the speculative prototype, Karma Kettle, weighing whether they wanted to use energy to boil water for a cup of tea, wait, store or sell excess energy back to the grid.

> A: I can also see that if you were in danger of falling at home … when you're in trouble if a connected devices senses that nobody has moved for a while and then automatically calls the help line.
>
> B: Well it would, if it gets it right ...
>
> C: So, if you've got a big house … big batteries. And you're away on holiday. Why shouldn't somebody else use the power … now that sort of holistic thinking would be marvellous.

At this point, participants were more interested in IoT functionalities than the data collected or the security of the technologies.

Later, participants were exposed to different volume and types of data collected by these domestic IoT devices, where the data collected were travelling to, geographically, and who is viewing their data, using a prototype developed by Associate Professor Max Van Kleek and his team [52]. To

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.

bring this matter closer to participants, they were asked to connect their mobile phones with the prototype, using WiFi connection, and observe where the data from their phone are going and to whom. This exposure shifted participants' articulated attitudes from a relatively balanced view, leaning more towards technological optimism, to increased scepticism. Participants began to question data-sharing practices, ethics and their consequences.

> D: It's very convenient, right? I mean I love it when Google maps knows where I'm going you … I don't mind if they know where I'm going, they'll work it out anyway …
>
> E: If you read *1984*, that is big brother watching you.
>
> F: They know when you're in the house … then have a map of when the lights are being used the most.
>
> G: It's just like when they do the terms and conditions … you don't really have a choice … and you don't know what you're signing up to … because they all wrap it up into some legal jargon ...

Here, the effectiveness of simulated scenarios began to manifest. The exposed data practices indeed triggered a mixed, emotional response, though shifting more towards the negative ones. This element of the intended functionality of the scenario prompted participants to draw a parallel between their immersive experience in the IoT home and their existing experience with other technologies with similar behaviours, concerning data. Participants' responses echoed degrees of increased confidence in critiquing complex and adaptive technologies, once they realised the similarity of the social consequences in the way the more familiar technologies and the emerging technologies like IoT operate. The persistent and dependent issues of privacy, safety, security, transparency and choice began to emerge, as participants continued their deliberation.

This awakening to the latent consequences of the data-intensive and connected features of IoT, even in the controlled (intended) scenario, prepared participants well for the scenario in which technologies failed. In this scenario, participants were exposed to three sequences of technology failure. First, as participants made themselves at home in their supposed living room, their Alexa Echo announced its acceptance of series of commands to lock down their living room door while opening their front door. Following that, a volunteer villain (one of the participants) entered the property and headed up to one of the bedrooms. Participants, locked in their own living room, watched the volunteer villain going through their supposed belongings, taking their valuables and leaving, from the live-feed of their Nest camera. Then, their Alexa Echo announced that it had accepted another command to purchase a holiday package to the Bahamas, chargeable to the bank account tied to the Amazon account.

These sequences of technology going wrong did not generate animated reactions. However, the substance of comments was serious. Participants' responses showed that the simulation helped them realise that what may appear to be benign functionality, data collection, processing and sharing could be abused, resulting in damage in real terms.

> A: Well, if they are monitoring it, and they know that you are now in the Bahamas, your house becomes vulnerable because they can simply hack into your system and remove all your furniture.
>
> B: That's a malfunction, isn't it? …
>
> F: Did the thief take your card to make a booking?
>
> G: It could have been hacked into, couldn't it? ... And that's why all of this data's got to be very carefully protected …

After the first two sequences of events, their Karma Kettle started switching itself on and off. This scenario heightened scepticism about the cyber-physical features of IoT.

> D: Well I wouldn't like that … my programme on my boiler … act[ed] up … a couple [of] years ago. And for about a year I ran it manually because the programmer wouldn't turn the under-floor heating pump on.
>
> E: So, you can't rely on electronic things … if there's WiFi involved … there's even more problems.
>
> D: And that's what worries me … One, you don't know absolutely when you press the button … it's going to work … Two, if you're not there and the boiler goes … if, you're not even there to check it … or … if you're in another country …

Again, these excerpts demonstrate the success of the simulated scenarios in prompting participants to draw on their subjective accounts of the familiar technology, to comment on the similar symptoms they are experiencing in the more complex, yet less visible operation of IoT. This enabled participants to construct a narrative about IoT technologies that they would not otherwise think they know enough to critique. Deliberation, with careful steering of the moderator, helped channel people's emotional responses towards reflective ones.

As participants moved from the experience sharing stage, their discussions began to concentrate on issues concerning:

- varying scope and scale of broken IoT security

> A: So, we have collapse of systems, national grid … what if … someone

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.

> hacks everyone's kettle at the same time … the whole national grid comes down … Or … what if it just malfunctions … whose fault is this … who's accountable …

- over-dependency on technologies

> B: … when you're looking at the demographic change …, increasing rates of dementia, I think that … people are going to be left behind …
>
> D: … in the future somebody will come into your house, and he will set up everything up for you, so it works hunky dory. He walks out the door, and two weeks later it all goes wrong. You've no idea how to fix it …

- technology complexity, the lack of interoperability and its consequences

> E: One of the things that we haven't talked about is how these things … do not interact with each other.
>
> F: It's only now that they are starting to realise that smart meters ain't that smart unless they work with all the other systems …

These concerns reflect values for security, responsibility, accountability, autonomy or degrees of independence and interoperability. Participants' discussions regarding over-dependency on technologies and the lack of interoperability imply their valuation of and interest in choice; their common concern was being locked in to particular products, services or providers. These values hint at priority areas for IoT security policies and design to respond to in order to continue realising the potential of and reaping benefits from IoT while minimising IoT risks and their consequences.

In brainstorming and shortlisting their responses to the problems, participants exhibited a strong sense of agency and value of responsibility. Participants' sense of agency was reflected in their preference for retaining degrees of control despite their interest in delegated human agency. Participants preferred to be able to opt in to the smart, connected features of domestic IoT. Control, here, manifests in people's freedom to decide, on demand, when to delegate their agency to technologies or associated agencies.

> A: It should be possible to come up with a list of defaults that are all switched off until you … switch it on … for the smart mode ...

Participants also recognised the need for 'a back-up plan'. This value manifests in their existing personal practices and preference to have a dual system – analogue/manual and digital. This served as both a preventive measure and a contingency plan.

> A: We take satnav, we take a map as well ... If you go walking in the hills, it's even more important to take a map … In case you run out of signal …
>
> B: … with the home, and this sort of smart technology surely it must be possible to have … a system that does everything most of the time, but the default, if it goes wrong, is that it goes back to manual.

In response to their concerns about interoperability, participants favoured the idea of standardising the connectivity element of IoT.

> C: I think standards is an important word … if this is gonna be a … a widespread thing, you're effectively introducing a new utility because the devices all vary. It's how they're connected that is universal ... It's a bit like, we've all got plumbing in our houses. We've got different looking radiators, different boilers, but the pipework and the connectors are all the same …

The way participants articulated this preference, drawing on their existing experience of managing utility systems in their house (e.g. plumbing and radiators), highlighted the success of the simulated scenarios in helping participants establish the connection between the way less familiar technologies and more familiar systems work. The deliberation provided a space for participants to translate their existing experience into solutions for what participants originally perceived to be unknown or unfamiliar technologies. Without this connection, participants are unlikely to get over the perceived, imposed knowledge barrier.

When it came to discussing responsibilities for addressing the problems participants identified, the debate became more flavoursome. Participants in both groups started off with an almost stern conviction concerning personal responsibility. This was already implied in their practices, for example, of taking a physical map, as well as a satnav on a car journey. However, as they recalled their immersive experience in the IoT Home, they realised that the options for them to exercise personal responsibility, for example by selectively switching on the smart features of domestic devices, were not available. Nor could they work out how Alexa ordered a package holiday and charged it to their bank account when they had not asked Alexa to do so. This realisation softened their conviction about personal responsibility. They started exploring the scope of responsibilities relevant entities should take.

> A: Need to keep control of things … that you're holding ...
>
> B: How would you change incorrect slash hacked data?

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.

> C: It's got to be manufacturers because they are in control of what they put before as the options for purchase.
>
> B: I would say researchers. What you're doing here … gaining knowledge from people that are … gonna be consuming your products …
>
> D: … Government have perhaps a responsibility for articulating the norms that we want to see adhered to, but … it's the manufacturers who have the responsibility for ensuring that these norms are adhered to in their products.
>
> B: I think there should be a panel that is representative from a wider section of society, to ensure that different groups are all included in that decision-making process.
>
> E: Well, it's two-ended, isn't it? One, … the supplier of the service, … like … you rely on the bank to have its own very powerful firewalls and … connection, protection and … encryption. So, you expect all that … but then you've got to do your own thing, as well.

Eventually, both groups came to the conclusion that individuals could not bear the responsibility of maintaining security on their own while grappling with fast-changing technologies. They deemed that individuals, companies, government and researchers are all responsible for making and keeping IoT safe for consumers and society. They also thought that the public should contribute to the configuration of responses to IoT security in policymaking and design development.

6 Conclusion

The deliberative process indicates varying shifts in people's value judgements. Participants moved from almost blissful complacency about the usefulness of the data-driven and networked features of IoT to questioning the consequences of its pervasive deployment. When presented with the scenario concerning technology failure, participants' scepticism about IoT security heightened. The scenario reminded them of similar problems that they had already experienced in the cases of web services and a broken boiler. This connection gave them the confidence to draw on relevant experience, channelling their initial emotional reactions to formulate responses.

This increase in confidence is also reflected in participants' articulated demands for participation in the ongoing development of IoT security policies and design. Compared to the pre-session survey result, in which 83% of participants reported that they had little to no influence over the way technology works, the recommendations that participants came up with suggested quite the opposite. The comparison between the pre- and post-deliberative survey results shows that 9 out of 14 participants who initially reported that they had little to no say over emerging technologies, like IoT, changed their mind about their efficacy to contribute to the development of emerging technology policies and design. Having participated in the simulated deliberation, participants across both groups reported that people should have a bigger say on how smart, connected technology works.

The shift in people's sense of efficacy demonstrates the potential of simulated deliberation to re-engage people in policymaking and design that traditionally privilege technical, objective knowledge over subjective accounts. Participants' recommendations and their increased enthusiasm to contribute to the development of data-driven and connected technologies highlights the strength of this approach in breaking down the knowledge barrier. As noted earlier, this knowledge barrier has traditionally hindered meaningful public participation, particularly, in policymaking for complex technology development and use.

The successful pilot implementation of this approach presents opportunities to scale-up the re-engagement of the public in the development of IoT security and other complex technologies across broader application domains. Increasing public participation in this way would allow a greater number of people to contribute to the construction of narratives concerning these issues. With the anticipated increase in diversity of value judgement in these narratives, it is likely that these technologies and their security will advance in ways that are more compatible with people's needs and capabilities.

7 Acknowledgements

The authors would like to express their appreciation to Paul Coulton (Lancaster University), Adrian Gradinar (Lancaster University), Max Van Kleek (University of Oxford), William Edwin Dixon (University of Edinburgh), Esteban Serrano (University of Edinburgh), Andrew Burton (BRE Smart Homes & Buildings), Susan Green (BRE Group) and BBC R&D for their contributions to PETRAS IoT in the Home Demonstrator.

8 References

[1] Ericsson: 'IoT connections outlook – Ericsson Mobility Report November 2018' (Ericson, 2018), https://www.ericsson.com/en/mobility-report/reports/november-2018/iot-connections-outlook

[2] DBS Group Research: 'Internet of Things: The Pillar of Artificial Intelligence' (Asian Insights Office, 2018), https://www.dbs.com/aics/templatedata/article/generic/data/e

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.

n/GR/062018/180625_insights_internet_of_things_the_pillar_of_artificial_intelligence.xml

[3] CISCO: 'CISCO 2018 Annual Cybersecurity Report: The attack landscape' (CISCO, 2018), https://www.cisco.com/c/en/us/products/security/security-reports.html

[4] Sivaraman, V. H., Gharakheili, H., Fernandes, C.N., et al.: 'Smart IoT Devices in the Home: Security and Privacy Implications'. IEEE Technology and Society Magazine, 2018, 37(2), pp. 71–79

[5] 'A cyber-attack could stop the country', https://www.bbc.co.uk/news/business-45952693

[6] 'Chalubo botnet wants to DDoS from your server or IoT device', https://news.sophos.com/en-us/2018/10/22/chalubo-botnet-wants-to-ddos-from-your-server-or-iot-device/

[7] He, H., *et al.*: 'The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing & other computational intelligence', Proc. Int. Conf. 2016 IEEE Congress on Evolutionary Computation (CEC), Vancouver, BC, Canada, July 2016, pp. 1015 - 2021

[8] 'Petya cyber attack: Chernobyl's radiation monitoring system hit by worldwide hack', https://www.independent.co.uk/news/world/europe/chernobyl-ukraine-petya-cyber-attack-hack-nuclear-power-plant-danger-latest-a7810941.html

[9] Maple, C.: 'Security and privacy in the internet of things', Journal of Cyber Policy, 2017, 2, (2), pp. 155 – 184

[10] Heer,T., Garcia-Morchon, O., Hummen, R. S., et al.: 'Security Challenges in the IP-based Internet of Things', Wireless Pers Commun, 2011, 61, (3), pp. 527 – 542.

[11] Rittel, H. W., Webber, M. M.: 'Dilemmas in a general theory of planning', Policy Sciences, 1973, 4, (2), pp. 155 – 169

[12] Head, B. W.: 'Wicked problems in public policy', Public Policy, 2008, 3, (2), pp. 101–118

[13] Head, B. W., Alford, J.: 'Wicked Problems: Implications for Public Policy and Management', Administration and Society, 2015, 47, (6), pp. 711 – 739

[14] Fischer, F.: 'Citizen participation and the democratization of policy expertise: From theoretical inquiry to practical cases', Policy Sciences, 1993, 26, (3), pp. 165 – 187

[15] Jasanoff, S.: 'Technologies of Humility: Citizen Participation in Governing Science', Minerva, 2003, 41, (3), pp. 223 – 244

[16] Heclo, H., King, A.: 'Issue networks and the executive establishment', Public administration: Concepts and cases, 1978, 413, (413), PP. 46 – 57

[17] Freedman, D.: 'The politics of media policy' (Polity, 2008)

[18] Domhoff, G. W.: 'Who rules America?: challenges to corporate and class dominance', (McGraw Hill Higher Education, 2010, 6th edn)

[19] Richardson, J. J.: 'Policy-making in the EU: Interests, ideas and garbage cans of primeval soup', in Richardson, Jeremy (Ed.): 'European Union: power and policy-making', (Routledge, 2006, 3rd edn.)

[20] Marsh, D.: 'Pluralism and the study of British politics: It is always the happy hour for men with money, knowledge and power', British Politics Today, 2002, pp. 14 – 37

[21] Marsh, D.: 'Understanding British government: Analysing competing models', The British Journal of Politics & International Relations, 2008, 10, (2), pp. 251 – 268

[22] Jordan, G., Richardson, J.: 'The British Policy Style or the Logic of Negotiation?', in Richardson, J. (Ed.): Policy Styles in Western Europe (Routledge Revivals), (Routledge, 2013).

[23] Coleman, S., Blumler, J. G.: 'The Internet and Democratic Citizenship: Theory, Practice and Policy' (Cambridge University Press, 2009)

[24] Hansard Society., 'Audit of Political Engagement 15 (2018)', 2018

[25] Schön, D. A., Rein, M.: 'Frame Reflection: Toward The Resolution Of Intractable Policy Controversies', (Basic Books, 1994)

[26] Fischer, F.: 'Policy Discourse and the Politics of Washington Think Tanks' in Fischer, F., Forester, J. (Eds): 'The Argumentative Turn in Policy Analysis and Planning' (Duke, 1993), pp. 21 - 42

[27] Hajer, M. A.: 'The Politics of Environmental Discourse: Ecological Modernization and the Policy Process' (Oxford University Press, 1995)

[28] Yanow, D: 'Public policies as identity stories: American race-ethnic discourse', in 'Telling Tales: On Evaluation and Narrative', (Emerald Group Publishing Limited, 1999, 1st edn.), pp. 29–52.

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.

[29] Isaacs, W.: 'Dialogue and the Art of Thinking Together: A Pioneering Approach to Communicating in Business and in Life' (Bantam Doubleday Dell Publishing Group, 1999, 1st edn.)

[30] Fischer, F., Gottweis, H.: 'The argumentative turn revisited: public policy as communicative practice' (Duke University Press, 2012)

[31] Hajer, M. A.: 'Deliberative Policy Analysis: Understanding Governance in the Network Society' (Cambridge University Press, 2003)

[32] Bloor, M. Wood, F.: 'Keywords in qualitative methods: a vocabulary of research concepts' (SAGE, 2006)

[33] Bradbury-Jones, C., Taylor, J., Herber, O. R.: 'Vignette development and administration: a framework for protecting research participants', International Journal of Social Research Methodology, 2014, 17, (4), pp. 427 – 440

[34] Yungblut, H. E. Schinke, R. J., McGannon, K. R. et al.: 'Understanding Physical Activity through the Experiences of Adolescent Girls', Women in Sport & Physical Activity Journal, 2012, 21, (1), pp. 3 - 14

[35] Gerard, N.: 'Can Millennials Talk About Death? Young Adults' Perceptions Of End-Of-Life Care', Journal of Health Administration Education, 2017, 34, (1), pp. 23 – 48

[36] Conrad, D. 'Rethinking "at-risk" in drama education: beyond prescribed roles', Research in Drama Education, 2005, 10, (1), pp. 27–41

[37] Coleman, S., Pothong, K., Weston, S.: 'Dramatizing Deliberation: A method for encouraging young people to think about their rights', Journal of Public Deliberation, 2018, 14, (1), pp. 1 - 5

[38] Pschtz, L., Pothong, K., Speed, C.: 'Autonomous Distributed Energy Systems: Problematising the Invisible through Design, Drama and Deliberation', Proc. Int. Conf. Weaving the Threads of CHI, Glasgow, Scotland, UK, May 2019

[39] Kuhl, M. E., Sudit, M., Kistner, J., Costantini, K.: 'Cyber attack modeling and simulation for network security analysis', Proc. Int. Conf. 2007 Winter Simulation Conference, Washington, DC, USA, December 2007, pp. 1180–1188.

[40] Moskal, S., Yang, S. J., Kuhl, M. E.: 'Cyber threat assessment via attack scenario simulation using an integrated adversary and network modeling approach', The Journal of Defense Modeling and Simulaion: Applications, Methodology, Technology, 2018, 15, (1), pp. 13–29

[41] McDonald, M. J. Richardson, B. T.: 'Position paper: Modeling and simulation for process control system cyber security research, development and applications Center for Information Management, Integration and Connectivity' (Center for Information Management, Integration and Connectivity, 2009)

[42] Kavak, H., Padilla, J. J., Vernon-Bido, D.: 'A characterization of cybersecurity simulation scenarios', Proc. Int. Conf. 19th Communications & Networking Symposium, Pasadena, California, USA, April 2016.

[43] 'Cyber ShockWave: Simulation Report and Findings', https://bipartisanpolicy.org/wp-content/uploads/sites/default/files/Final%20Cyber%20Brochure.pdf

[44] Gallaher, D.: 'Cyber simulation lessons learned' (TAG Information Security, 2015), pp. 1 - 6

[45] 'BBC Breakfast', https://www.bbc.co.uk/programmes/b0c2jj8d

[46] Dunne, A., Raby, F.: 'Design Noir: The Secret Life of Electronic Objects' (Springer Science & Business Media, 2001)

[47] Michael, M.: '"What are we busy doing?" Engaging the idiot?', Science, Technology, & Human Values, 2012, 37, (5), pp. 528–554

[48] Dryzek, J. S.: 'Democratization as Deliberative Capacity Building', Comparative Political Studies, 2009, 42, (11), pp. 1379–1402

[49] Mansbridge, J. *et al.*: 'A systemic approach to deliberative democracy', in Parkinson, J., Mansbridge. J. (Eds.): 'Deliberative Systems: Deliberative Democracy at the Large Scale' (Cambridge University Press, 2012), pp. 1 - 26

[50] Coleman, S., Przybylska, A., Sintomer, Y. 'Deliberation and Democracy: Innovative Processes and Institutions' (Peter Lang, 2015)

[51] Steiner, J.: 'The Foundations of Deliberative Democracy: Empirical Research and Normative Implications' (Cambridge University Press, 2012)

[52] Van Kleek, M. *et al.*, 'X-Ray Refine: 'Supporting the Exploration and Refinement of Information Exposure Resulting from Smartphone Apps', Proc. Int. Conf. 2018 CHI Conference on Human Factors in Computing Systems, New York, USA, 2018, p. 393

Authorized licensed use limited to: UNIVERSIDADE ESTADUAL DE MARINGA. Downloaded on July 02,2025 at 13:21:05 UTC from IEEE Xplore. Restrictions apply.