Privacy for IoT: Informed Consent Management in Smart Buildings

Chehara Pathmabandu[a,b], John Grundy[a], Mohan Baruwal Chhetri[b], Zubair Baig[c]

[a] *Faculty of Info. Tech., Monash University, Australia*
[b] *CSIRO's Data61, Australia*
[c] *School of Info. Tech., Deakin University, Australia*

Abstract

Smart Buildings (SBs) employ the latest IoT technologies to automate building operations and services with the objective of increasing operational efficiency, maximizing occupant comfort, and minimizing environmental impact. However, these smart devices – mostly cloud-based – can capture and share a variety of sensitive and private data about the occupants, exposing them to various privacy threats. Given the non-intrusive nature of these devices, individuals typically have little or no awareness of the data being collected about them. Even if they do and claim to care about their privacy, they fail to take the necessary steps to safeguard it due to the convenience offered by the IoT devices. This discrepancy between user attitude and actual behaviour is known as the 'privacy paradox'. To address this tension between data privacy, consent and convenience, this paper proposes a novel solution for informed consent management in shared smart spaces. Our proposed Informed Consent Management Engine (ICME) (a) increases user awareness about the data being collected by the IoT devices in the SB environment, (b) provides fine-grained visibility into privacy conformance and compliance by these devices, and (c) enables informed and confident privacy decision-making, through digital nudging. This study provides a reference architecture for ICME that can be used to implement diverse end-user consent management solutions for smart buildings. A proof-of-concept prototype is also implemented to demonstrate how ICME works in a shared smart workplace. Our proposed solution is validated by conducting expert interviews with 15 highly experienced industry professionals and academic researchers to understand the strengths, limitations, and potential improvements of the proposed system.

Keywords: IoT, Smart Buildings, Informed Consent, Privacy Preservation, Nudging, Compliance

1. Introduction

By 2025, the total number of connected IoT devices are predicted to reach 75.44 billion, representing a three-fold increase compared to 2019 [1]. These IoT devices and systems – mostly cloud-based – form the foundation for smart buildings (SBs) that span across multiple domains, including office spaces, hotels, hospitals, malls, shopping complexes, restaurants, and other commercial or residential spaces. Advanced IoT-based solutions enable SBs to monitor and collect extensive data about the peoples' presence and movement on the premises across space and time. This data is used by SBs to contextualise and self-regulate operations, and set up more efficient workflows according to the occupants' diverse needs, preferences and feedback [2]. However, existing data collection practices are still very siloed and the devices capture data directly related to individual inhabitants, making it difficult to preserve and protect individual privacy. This increases the possibility of sourcing and integrating personal identifiable information (PII) about occupants from multiple places to identify them. Personalised behavioural patterns can be learnt by combining the data collected by such IoT devices in distributed settings, often without the knowledge and consent of the SB occupants [3]. Given this extensive collection of data and the resulting potential for privacy risks, there is an increasing need for greater transparency and end-user awareness about data collection practices in SBs [4].

Although people express concern about the privacy of their data collected from smart devices [5], research shows that the convenience offered by these devices influences their privacy-related behaviours, and they rarely make active efforts to protect their personal information. instead allowing themselves to be monitored [6]. This phenomenon is referred to as the *privacy paradox*. People are typically poor at assessing potential privacy risks or violations and their personal experience may directly affect the privacy decision-making process as they tend to exaggerate or neglect hazardous situations [7]. Also, controlling digital privacy is surprisingly complex and time-consuming and people may lack the expertise required to manage the technical aspects of privacy protection [8]. In particular, the privacy policy documents that are attached to the IoT devices, and set out what the service providers will do with the user data, are lengthy and complicated. These policy documents and contracts are often written for a combination of smart peripherals offered by the same provider, thus challenging the user in differentiating and understanding respective terms for each purchased device. Moreover, given the strict requirements of the General Data Protection Regulation (GDPR) [9], the provision

Email addresses: chehara.pathmabandu@data61.csiro.au (Chehara Pathmabandu), edlisle@bigpond.com (John Grundy), Mohan.BaruwalChhetri@data61.csiro.au (Mohan Baruwal Chhetri), zubair.baig@deakin.edu.au (Zubair Baig)

of legally sufficient consent for data collection is becoming increasingly difficult.

There are a number of conditions for the validity of consent including: it should be freely given, and be specific, informed and unambiguous. In some cases, smart building IoT solutions cross-jurisdictional regulatory boundaries and blur the notion of private and public, e.g., data is collected in one continent but hosted on a cloud in another continent. Therefore, there is a real risk that the data collected by smart devices is shared and retained in transit by a variety of external parties (Government, Data brokers, Service providers, Manufacturers, etc.) without explicitly informing the users [10]. Processing personal data is generally prohibited unless it is expressly allowed by law or the data subject has given consent. As the navigation of IoT technology itself can be daunting, and the relation with digital services is bound by complex terms, conditions and privacy policies, there is a growing necessity for improving the way in which legal consent is sought for the capture and use of user data. Moreover, the context for consent can change as the inhabitants go about their daily activities in a smart environment (e.g., shared office space environment or personalised smart home environment).

To address this problem of consent and privacy management in IoT-enabled Smart Building (SBs), a user-centric *Informed Consent Model* (ICM) is proposed by the authors that (a) enhances visibility into data collection by smart devices without forcing users to understand lengthy policy statements, and (b) increases the users' awareness about the privacy implications of the data collection practices, while (c) nudging them to make more informed decisions about consent or refusal. We develop a reference architecture for building an *Informed Consent Management Engine (ICME)* to assist software developers in designing and implementing diverse end-user consent management solutions for SBs. We implement a proof-of-concept prototype to demonstrate how ICME can be realised in a shared smart workplace. We also conduct an interview study with experts to understand the strengths, limitations and potential improvements of ICME.

This paper makes the following key contributions:

- *Identify the key data privacy and consent requirements for IoT-based SBs;*
- *Propose a new reference model and architecture for informed consent management in SBs;*
- *Implement a proof-of-concept prototype for a shared smart workplace; and*
- *Validate the proposed approach with 15 highly experienced industry professionals and academic researchers.*

The rest of the paper is organised as follows. Section 2 presents an overview of related work in the area of data privacy, informed consent and digital nudging in the context of SBs. Section 3 details the motivation and research methodology used in our study. Section 4 and Section 5 present our design of ICME including the proposed user-centric informed consent model and reference architecture, and prototyping efforts within a smart office. Section 6 details the validation process of ICME through expert interviews along with the key insights from data analysis. Section 6.7 concludes the paper.

2. Background and Related Work

2.1. Data Privacy and lengthy privacy policies

The concept of privacy and personal identifiable information (PII) is diverse, depending on whether a person can be identified or reasonably identifiable under certain data aggregation procedures. Clarke defines privacy as "the interest that individuals have in sustaining a 'personal space', free from interference by other people and organisations" [11]. Maslow has identified the "need for privacy" as a core property of self-actualization, which is the highest level of psychological development [12]. A more comprehensive interpretation of privacy includes all aspects of an individual's social needs so that privacy can be categorised as *privacy of person*, *privacy of personal communication*, *privacy of association, behaviour and action*, *privacy of thoughts and feelings* and *privacy of personal data – image, location, space* [13].

According to the GDPR [9], and many other associated laws, including the Australian Privacy Act (APA) [14], Health Insurance Portability and Accountability Act (HIPAA) [15] and Personal Information Protection and Electronic Documents Act (PIPEDA) [16], individuals have the right to control their own data and not have their transactions linked or tracked through IoT devices. For instance, in smart healthcare facilities, patient medical documents must remain confidential, except when there is a necessity for legitimate access to these records. However, some controversial insights on data privacy can be identified from Courtney's seminal work on Smart Residential Care Facilities [17], where privacy concerns of the seniors are reduced when the smart devices are used only for medical intentions or in the case of a potential emergency.

Recent research works have shown that lengthy full-text policies cause problems in the comprehension and retrieval of required information by end-users. Researchers have proposed different solutions to address this problem including implementing a textual pattern-based approach [18], a labelled grid layout [19], and symbolic visualization [20]. They have also proposed various tools [21] and policy editors [22] for the generation of privacy policy statements. These solutions aim to improve the comprehensibility of the text in privacy policies and address the incompleteness of the information presented to the end-users with respect to privacy practices.

2.2. Personal Data Usage and Informed Consent

While *consent* is frequently used as a justification for businesses to use and disclose personal information, valid consent goes beyond clicking the 'I agree' button. Consent increases user awareness, gives consumers a chance to limit access to their data and promotes safer data practices. According to the Australian Privacy Principles (APP) Guidelines, meaningful consent has the following five aspects – *capacity*, *voluntary*, *current and specific*, *informed* and *expressed* or *implied* [23]. An individual, or a guardian in the case of a minor, must be capable of giving consent for it to be valid (*capacity*). Consent

must be a genuine choice that is freely given (*voluntary*). For instance, forcing workers to wear IoT wristbands to monitor their performance [24] or placing chemical sensors on doctors to ensure they wash their hands enough [25] cannot be considered voluntary consent. Consent must be specific to an identified purpose and cannot be assumed to last indefinitely (*current and specific*). An individual must have a full understanding of all applicable details for their consent to be meaningful (*informed*). Finally, the consent must be expressed orally or in writing to be valid (*expressed or implied*).

2.3. Data Privacy and Smart Buildings

The modern data collection practices in IoT ecosystems have introduced several new privacy challenges. In the context of smart environments, they include *obtaining consent for data collection, allowing users to control and choose the data they share, and ensuring that the use of collected data is bound to the declared purpose* [26]. These challenges get even more complicated due to the increased potential for misusing sensitive information in the IoT environment, arising from the pervasive tracking of habits, behaviours, location history and presence or absence over a long period [27].

With people being surrounded by a growing number of smart sensors, it is challenging to express their privacy consent choices electronically. Most of the devices used to collect data in IoT-oriented smart building environments have limited resources, are battery-operated or are passive, i.e., without any user interface [28]. Given the difficulty of providing informed user consent for smart peripherals, consumers are willing to trade away their privacy due to unawareness of the amount of privacy that is being lost [26]. It increases the *privacy paradox in IoT* as there is an inconsistency between people expressing privacy concerns but continuing to use these devices that have significant potential for eroding their privacy [8]. Recent studies have described the conflict between the need for personalisation and the concern over personal privacy as the *Personalisation–Privacy: P-P Paradox in IoT* [29].

Although people are concerned about the negative consequences of excessive disclosure of personal information, and their trust decreases after seeing the evidence of the loss, research shows that they gradually return to the original state, engaging in privacy-sacrificing behaviours [30]. Several solutions seek to improve this situation by managing access control and permissions granted by the user to IoT devices, e.g., AppOps [31] and Norton AppAdvisor [32]. Both applications directly fetch and analyse OS-level permissions and allow users to selectively grant or deny permissions for installed apps. These apps highlight privacy risks associated with a specific type of sensitive information (e.g., location information). Also, they send notifications, including a detailed report of the privacy risks associated with the app. However, in contrast to our work, neither compares the compliance of IoT data payloads with the agreed privacy policy statements to detect any breaches.

Researchers have demonstrated how a low-cost Raspberry Pi-based device can warn users when a voice assistant snoops on people without their consent and being woken up [33]. While their work focuses on voice assistants and checks the sudden increase of traffic rates in audio-related events, our approach can be applied to any smart device and scenario by checking all payloads for any user-triggered event. Also, they do not consider checking the policies related to the audio recording of the device while our solution scans all the events with the defined policies of the device.

2.4. Nudges and End-user Privacy Behaviour

Digital nudging is a concept used to influence the privacy behaviour of users.*Protection Motivation Theory* (PMT) [34] proposes that people conduct two appraisal processes when facing a threatening event: one focused on the threat itself, and the other on the options to diminish it. This approach affects a user's intention to take preventive action and results in adaptive or maladaptive behaviours [34]. Framing of content in a message can considerably affect the user behaviour. According to principles including loss aversion and the endowment effect, the pain of losing something is greater than the joy of getting it. Similarly, people will take risks when dealing with potential losses but avoid them when dealing with potential gains [35]. E.g., when using smart technologies, the user needs to perform a risk-benefit analysis to decide whether or not to disclose their personal information while using the service. According to the privacy calculus theory, individuals tend to exchange their personal information for time and money, self-enhancements, or pleasure [36] confirming the *privacy paradox* concept.

End-user privacy behaviour can also be influenced by factors such as herd mentality [37] and social norms [38]. Social norms refer to how an individual believes that others expect them to behave [38]. Social norms emanate from a small group of known individuals, such as family members, coworkers, or close friends, and are expected to judge the adoption decision as they care how using a certain technology will influence the image in their social circle. On the other hand, herd behaviour typically includes complete strangers. Those exhibiting herd mentality, do not greatly care about how the people they follow will judge them for using certain technology and might not even know about their choices [37].

3. Motivation and Research Methodology

The paper first presents a motivating scenario of a voice-enabled workplace to illustrate some of the challenges related to privacy and consent management in SBs. The key research questions and the methodology used to answer them are then presented.

3.1. The future of work: A voice-enabled Smart workplace

In voice-enabled smart offices daily activities are automated, linked and personalised by leveraging advances in IoT and AI to increase productivity and enhance user experience. Examples include finding the closest parking lot, accessing the indoor maps to book a working desk, adjusting the lighting and heating settings, reserving a meeting room in advance, controlling multiple user access by integrating with the calendar system, locating colleagues, etc. Fig. 1 illustrates the typical services that an individual working in

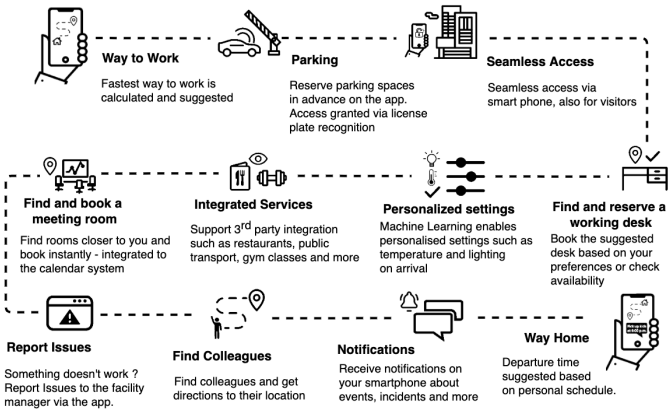

Figure 1: Example of a Voice-activated Smart Office

a smart workplace would use and interact with on a daily basis. However, to provide such personalised, user-centric services, multiple system components, sensors, smart IoT devices, actuators and voice assistants must be interconnected to capture user data consistently. Voice-based digital assistants are fast replacing touch as the primary user interface in many such environments [39]. New speech recognition technologies have simplified the execution of voice-activated commands by improving the ability to speak contextually and naturally to an electronic device or a computer system.

As voice-enabled devices become increasingly integrated into our homes, workplaces (see Fig. 1), and daily routines, the ubiquity of such internet-connected devices raises many concerns around privacy and trust. Voice-activated devices can be classified as *manually activated*, *speech activated* or *always on* [40]. Of these, the *always on* devices have the highest levels of privacy concerns as they operate silently in the background while continuously recording and transmitting data associated with human activities and behaviours. The primary purpose of continuously capturing inhabitant data (e.g. presence, behaviour, preference, etc.) is to enhance user experiences with minimal disruption while operating in the background as part of the living environment. Consequently, *individuals frequently interact with "smart devices" without even realising that they exist in the environment and without any visibility into what data these devices are collecting and how they are (re-)sharing them downstream*. In addition, smart appliances including light bulbs, smart switches, door locks, indoor cameras, and many other devices [41][42] bring along diverse privacy concerns and challenges that extend beyond the privacy boundaries into other dimensions. Some of these challenges are discussed further that act as motivating factors for *informed consent management*.

3.2. Key Challenges Related to Data Privacy and Informed Consent in Smart Buildings

Monitoring and controlling the data collected by the ever-growing number of smart, connected devices are becoming more challenging for SB occupants [43]. Challenges faced by users of smart devices are presented below.

3.2.1. Incorrect mental models of IoT data capture and usage

People often form inaccurate mental models of how smart devices operate in SB environments. For instance, users have trouble understanding/explaining the system based on their mental model when they have to deal with binary states of the system (e.g. locked or not), order of the priorities, judging the functionality and mixing of sensor events or interrupts (alerts) [44]. This is largely due to the complex nature of interactions among connected smart devices, components, organisations and third parties. As a result, users often make poor privacy decisions and give non-meaningful consent to the data associated with their interactions with smart devices, violating the principle of valid consent. Some possible reasons include not being fully aware of the device features and their privacy implications, product unfamiliarity, poor usability and complex privacy policy documents [8]. The extensive use of technical terms in many privacy policy documents makes it hard for users to understand the purpose of data collection and to link the interactions with applicable policy statements. In particular, many people still do not read the privacy policies and the Privacy Policy Agreement (PPA) for IoT devices (which may differ considerably from the website PPA) [45].

3.2.2. Unethical collection, use and disclosure of individual and collective IoT data

IoT data has the potential to reveal highly sensitive information about users. E.g., consolidating data from multiple sensor sources including temperature, humidity, light level and CO2 of a room can track its occupancy with considerably higher accuracy than with data from only one source [46]. Some of the insights gained from the analysis of such data are beneficial for marketing, service provisioning and optimising natural resources within SBs. However, unethical data collection and usage may have profound privacy implications in smart spaces. In 2015, privacy advocates lodged a complaint with the Federal Trade Commission (FTC) in the US against Samsung's microphone-enabled Smart TV stating that it was *always switched on* in violation of federal wiretapping laws [47]. This complaint appeared after users noticed that Samsung's Privacy Policy provided a warning that "sensitive conversations might be picked up and transmitted to third parties" as part of the TV's voice-controlled search function. As another example, many organisations use smart electricity meters that are capable of obtaining potentially sensitive data about the occupants, including activties carried out in the smart space [48].

3.2.3. Limitations of de-identification of IoT data to protect individual privacy

De-identification is the process of removing identifying information from collected or produced data. It prevents someone's personal identity from being revealed to preserve privacy. However, data collected by the IoT components in SBs is often very difficult to de-identify due to its highly granular nature. For example, an individual can be uniquely identified out of 1.5 million anonymised mobile-phone location streams [49]. Sensor-based devices capture a unique, rich picture of an individual, with many related activities. They often permit

profound and unexpected inferences about personality, character, preferences, and intentions. Therefore, it is important to keep individuals anonymous by avoiding collecting information that can identify them and making any such data challenging to identify throughout the IoT data lifecycle [50]. However, advanced ML classifiers and AI models can be trained to infer sensitive information from data sets, e.g., in acquiring trade secrets from a competitor's equipment, potentially violating intellectual property rights [51].

3.2.4. Immature IoT solutions with poor privacy controls

Many IoT devices are manufactured for personal use in close proximity, and they capture sensitive data related to the user. Any collated personal data is beneficial to assist manufacturers or vendors improve their products. It has been found that most manufacturers and vendors do not have adequate privacy policies for their IoT devices and there is a potential of lower compliance with their PPA statements [45]. Therefore, service providers may collect more data than what is required from users, and often devices with no user interactivity may generate a great amount of invisible data as they do not facilitate user consent (e.g., electricity or water sensor, connected oven or appliances, tracking devices, or other IoT sensors that do not have input and output capabilities). In addition, vendors frequently prioritise ease of use, novel functionality, and quick time to market, paying less heed to privacy risks [52].

3.3. Research Questions and Approach

Three key research problems that require further research in the domain of privacy and consent management in SBs have been identified. The following three research questions(RQ) are formulated respectively to address them:

- *RQ1: What is an appropriate model for informed consent and privacy management in Smart Buildings to support stakeholders in implementing better privacy controls while enhancing an individual's ability to obtain more granular transparency?* Examination of the literature shows that there is a lack of informed consent around *data capture and usage* and *user awareness of data disclosure* in smart buildings. Example requirements to facilitate informed consent include the need for a clear definition of (i) how PII is collected, used, shared and disclosed, (ii) how permission is sought and granted for the accumulated data to be shared and disclosed to third parties, and (iii) what are the liabilities related to any breaches of private information. As a solution, a novel user-centric *Informed consent Model (ICM)* for SBs is proposed that will enhance the standard IoT infrastructure to control the privacy of data circulation across cloud platforms, underlying services and beyond.In answering RQ1, we consider providing visibility into privacy policies against infringements by IoT devices to positively influence the privacy behaviours of users.

- *RQ2: What is a suitable reference architecture that supports the development of consent and privacy management systems for Smart Buildings?* We propose a *reference architecture* for implementing consent and privacy management systems based on the above proposed ICM. This reference architecture can serve as a blueprint for implementing diverse end-user consent management solutions for a variety of shared smart spaces. This study also provides a proof-of-concept prototype for a shared smart workplace to demonstrate its feasibility and practicability. E.g., It explores ways to (a) capture IoT data attached to outbound events, (b) apply different technical solutions for ICM to handle user consent, and (c) design a specific implementation for the proposed architecture for controlling sensitive data disclosure. The reference architecture, implementation, and prototype are collectively referred to as the 'Informed Consent Management Engine (ICME)'. ICME supports multi-user, multi-device setups as well as different hierarchical setups in smart spaces to enhance user awareness.

- *RQ3: How can we validate the proposed approach and examine its effectiveness (including strengthes and limitations) in managing informed consent in SBs?* We evaluate the usefulness of ICME (from RQ2) by conducting an expert interview study following three assessment conditions. Practical, methodological and conceptual assessment conditions are examined to investigate the impact of ICME in enhancing the privacy practices of IoT. It also seeks expert opinion to address the technical issues raised by ICME due to forced assumptions and suggests ways to better understand privacy-preserving practices in conjunction with existing methods. The paper also inspects how the design decisions deviate or conform from end-user expectations on data collection and usage from an expert eye by taking them through an actual case study in a simulated environment.

3.4. Research Methodology

This study was conducted using three scientific research methods including modelling, prototyping and surveying. Each research method supported the research in answering the respective research questions detailed in Section 3.3.

3.4.1. Modelling study

Following a systematic literature review, we identified a set of key requirements for informed consent in SBs to address ambiguity in (a) how IoT devices are complying with their privacy policy statements following user consent for various access permissions, and (b) the extent to which users have visibility and awareness of their data collection and use. Based on these requirements, a user-centric Informed Consent Model (ICM) for SBs is developed. The ICM model redefines the formal structure of data flows in an IoT network-based SB, verifying individual privacy policy statements' compliance attached to smart devices. In addition, a reliable methodology is devised for privacy and consent management based on the ICM model.

3.4.2. Feasibility study

To demonstrate the feasibility of the proposed solution, a proof of concept prototype has been implemented as the *Informed consent Management Engine (ICME)*. It employs the ICM model for the management of consent in smart working

spaces. The prototype was implemented in a simulated environment primarily using a Cloud API server, Document database server, Push notification service, hardware-API writing tool, IoT dashboard, device interfaces and a mobile application. Several use cases were designed around a voice-activated smart office space where multiple users, smart devices, data flows, privacy settings, and permissions are integrated.

3.4.3. Expert Interview study

We conducted an expert interview-based study to evaluate the ICME prototype to identify the strengths and limitations of the proposed solution. 15 highly experienced experts in the area of Privacy, IoT and SBs were recruited through a rigorous screening process. The study was conducted after getting the necessary ethics approval and following the basic principles of ethical research. Due to COVID-19, the interviews were conducted remotely with all participants.

4. Informed Consent Management Framework

This section briefly discusses the key requirements for informed consent in smart buildings. Next, our proposed ICM model and its process are presented followed by a reference architecture for ICM Engine.

4.1. Key Requirements for Informed Consent

The following key requirements for obtaining informed consent in SBs were identified through detailed literature analysis.

- When activating permissions to consume "smart services", determine for each smart device what data it collects, how, when, and what privacy implications this may have;
- Label collected data as sensitive and non-sensitive, e.g. change in room temperature may unintentionally reveal a person's presence;
- Record existing privacy settings and data sharing practices of each user and use them to provide them ongoing awareness;
- Address relevant privacy by design (PbD) principles;
- Structural representation for privacy policies, i.e., define the user, team, and organisational privacy policies in the presence of the smart devices;
- Revise dynamic/ongoing consent, i.e., as the user moves around in the smart space, new devices are encountered, data capture begins/changes, the new user enters a room, etc.;
- Ensure the maintenance of meaningful informed consent, i.e., when a new/changed/integrated device is capturing unintended data, proactively highlight it for users to ensure their valid consent;
- Provide multi-user and multi-device support in shared smart environments.

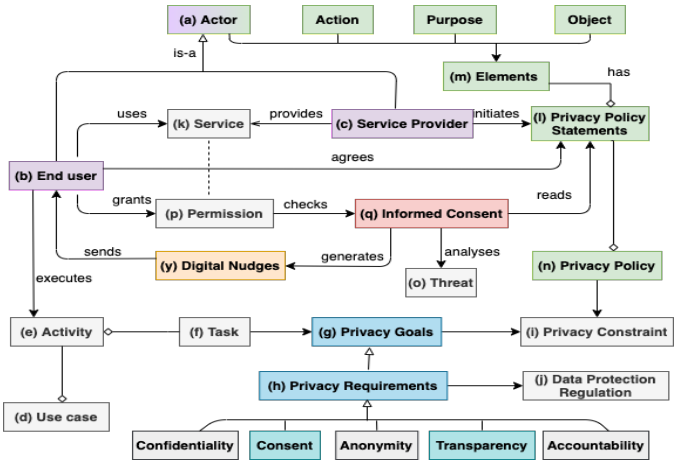

Figure 2: Informed Consent Model (ICM) for Smart Buildings

4.2. Informed Consent Model (ICM)

To satisfy the above prerequisites, a conceptual model for informed consent [53] is proposed, as shown in Fig. 2. There are two key *actors (a)* involved in our consent model – the *end-user (b)* and the *service provider (c)*. Both actors may depend on each other for accomplishing their objectives (e.g. communication and exchange of messages). The end-user executes multiple *tasks (f)* associated with the device-specific *activities (e)* related to a particular *use case (d)*. E.g., an employee may unlock the smart lock on the front door of the smart office via his voice assistant or digital card. After finding a free desk space, the employee may adjust the brightness of the smart lights to meet his preferences with a single command (refer to the scenario presented in Section 3.1).

A set of *privacy goals (g)* has to be fulfilled when executing the service provider-defined tasks (e.g. unlinkability, intervenability). These goals represent an intention to mitigate threats and limit harm to personal information by satisfying privacy criteria concerning such information. *Privacy requirements (h)* are used to capture the data subject privacy needs at a high level of abstraction in conformance with the *data protection regulation (j)*. Referring to the example in Section 3.1, employees have the right to know whether their personal preferences, working hours, and entry and exit times are monitored or tracked from their daily interactions with the smart devices. Furthermore, the privacy requirements can be further classified as *Confidentiality*, *Consent*, *Anonymity*, *Transparency* and *Accountability*. Although all factors are equally important, we focus mainly on enhancing user consent and transparency throughout the data life cycle.

End-users (b) consume the *service (k)* provided by the dedicated *service providers (c)* of the smart devices. All the applicable *privacy policy statements (l)* of these devices are initiated by their service providers and should align with applicable data protection laws and regulations. These privacy policy statements are mostly found during the installation and update of an IoT device, or progressively with the usage of different features offered by the service provider. For example, an employee may grant access to his calendar schedule to facilitate

multiple access to a meeting room and to assist with advanced reservations based on the participant's capacity.

Furthermore, the way an IoT device functions can change gradually over time. For instance, the features present when the device is first bought may be updated or replaced with newly introduced features at a later date through upgrades (e.g. turning Nest Secure's keypad hub into a Google Home Mini) [54]. An IoT vendor might be acquired by a different organisation that has an entirely different set of privacy policies. It may then collect and use PII for new purposes that current users may not have contemplated (e.g. Google's Policy with Fitbit Data) [55].

Long privacy policies have been shown to be unhelpful for end-users to retrieve required information (See Section 2.1). So, privacy policy statements are partitioned into four *elements (m)* as presented in Fig. 2. *Employees (b)* who have consented to share their sensitive information should have visibility into (i) who monitors, collects, and uses their data, and (ii) the right to withdraw their consent at any time.

The *threats (o)* capture events that can potentially threaten PII by misusing such information. Based on the severity of the impact, threats can be characterized as high, medium or low. A threat can also be either natural, accidental, or intentional. Referring to the example in Section 3.1, analysing an employee's data over time may reveal insights into working patterns, personal habits, power consumption, medical conditions, search history, social connections and presence which may cause a potential gateway for intentional threats.

Privacy conformance checking is done by intercepting the device API calls and checking the list of permissions requested by a device (and granted by a user) against the device privacy policies. When the *end-user (b)* triggers an action, and *permission (p)* needs to be granted to a *service (k)*, the *informed consent engine (q)* checks the permissions granted by the user and the event's payload data against the device's privacy policy statements. If the consent engine detects a policy infringement, the end-user is made aware of it through a *digital nudge (r)* and recorded to maintain the event history for future use. Following the nudge, the user can decide if they want to take appropriate actions against the infringement, such as not using the device, refusing permission for data capture, or leaving the smart space.

4.3. Application of Privacy by Design

In designing our proposed SB informed consent model, we have addressed five out of the seven foundational principles of *privacy by design* (PbD) [56]:

1. *Proactive, not reactive; preventative, not remedial* – Privacy considerations must help drive the design, and not the other way around wherein the design process leads to the detection and highlighting of privacy violations. Our proposed consent model creates an environment for the end-user to take proactive actions to control the disclosure of their data, limiting potential privacy infringements.
2. *Privacy as default setting* – Activities that exceed the expected data privacy context must require the affirmative informed consent of the individual. Here, understanding the default context is about understanding the tacit context between participants. The proposed consent model performs a cross-check of the access permissions granted by the user with the privacy policies of the IoT devices. It ensures that no smart device exceeds the contextual understanding of the parties that the default privacy policy has been violated, a novel aspect of this research compared to any existing research.
3. *Privacy embedded into design* – Privacy must be inseparable from the design so that the system or process would not function without privacy-preserving functionality. Our proposed solution implements this principle by requiring that all events of the connected devices must go through the consent model as a safety feature.
4. *Visibility and transparency* – Pushing consent-seeking "nudges" to the end-user with a full justification about the collection or use of PII increases visibility. This information helps the user decide whether to grant permission to service, moderate their behaviour or use the model-recommended corrective actions to reduce privacy risks.
5. *Respect for user privacy by keeping it user-centric* – Every user is different in terms of their privacy expectations. This principle states that each user should have the ability to define their own privacy expectations, e.g., for work context, location, set of devices, time of day, activity etc. Our approach allows this.

4.4. Informed Consent Management Process

Smart buildings can house many *organizations* spread across multiple *floors* and occupying many individuals and shared *rooms* that can be grouped into different *zones*. Each of these "smart spaces" may be instrumented with different types of devices that are shared by multiple users with different levels of accessibility, authority, and privacy preferences. The nudging mechanism used and the nudging content presented to the inhabitants of these smart spaces may differ significantly depending on their level of accessibility and authority. A central concern in managing such *system of systems* is the complex relationship between the smart spaces, shared devices, and their users. Below, we describe a five-phase process for managing the privacy of the inhabitants in dynamic shared smart spaces, i.e., when new users join the building, or new devices are added to the system.

- *Phase 1: Extract privacy policies by applying textual patterns.* Privacy policies and consent-related documents are often lengthy and complicated to read, causing cognitive overload for device users. Therefore, for each device installed in the shared smart space, its privacy policies are extracted based on a pre-defined textual pattern, converted into an appropriate machine-readable format (e.g., JSON, XML), and stored in a *privacy policy document database* (PDD). As shown in Fig. 3, each privacy policy statement has the following elements: Actor, Action, Object(s), Purpose(s) [18], e.g. *the service provider collects end-user usage frequency for service provisioning/analytics*.

Figure 3: Extracted privacy policy statements in a textual pattern - objects of objects representation on MongoDB Document Database

- *Phase 2: Maintain a list of risky permissions for smart devices.* A *PII bank* is created to maintain a list of sensitive and non-sensitive user information that may be collected and transferred when users interact with devices in the shared smart space. Each PII type is linked to a risk level based on its sensitivity, e.g. *a user's precise location is highly sensitive compared to an approximate location*. Each time a new device is installed in the shared smart space, all permissions (mandatory and optional) defined by the device's manufacturer are checked to gain more visibility into the personal data that the vendor can collect about the device user at both the software and hardware level. Following this, possible dangerous permissions that have the risk of revealing sensitive information about the users and could be used for profiling, tracking, advertising and identification [57] are identified, labelled and listed. Each policy statement extracted in Phase 1 includes such PII types under the object element.
- *Phase 3: Check for privacy breaches or potential risks when users interact with devices.* Every time a user interacts with an SB's smart device, the payload data for the user-executed action is captured by ICME and pre-processed into a machine-readable lightweight data-interchange format. This payload is then assessed against the privacy policy statements for that device stored in the PDD. More specifically, the PII types under the object element of the privacy policy are compared against the parameters collected in the payload. To achieve this, it is expected to develop and deploy APIs of ICME with a document database connection to check whether each payload fails to meet the privacy policies. Two types of incidents are flagged – *direct breach of the privacy policy* and *potential disclosure of high-risk PII*, even if no direct infringement is identified.
- *Phase 4: Track and log events associated with privacy breaches or potential risks.* Once a smart device's payload has been assessed against its privacy policy statements, the user-triggered action (event, action, time, current status) is tracked and logged for all incidents flagged in Phase 3.
- *Phase 5: Recommend corrective actions using nudges.* The incidents logged in Phase 4 are used to recommend corrective actions to the user via nudges to control and mitigate emergent privacy issues that have occurred and/or may transpire in future. Nudging is an approach for influencing people's judgment, choice or behaviour in a desirable way and is used in a range of domains including cybersecurity [58]. In designing the nudge content, we have considered the concepts of protection motivation theory (PMT) [34], herd behaviour [37], social norms [38], privacy paradox [8] and privacy calculus theories [38] to enhance user awareness, share good practices, and to motivate users to review and possibly adjust their privacy settings. In our approach, a nudge consists of three elements: (1) a summary of the unauthorised actions, (2) two options for ignoring or allowing data to be shared, and (3) redirecting instructions to the privacy settings window. After the initial step of generating the simplified terms and conditions, the consent engine will progressively ask consent to capture, process or share data in a way that the user can understand the consequences. In addition, sending personalised privacy protection nudges based on user preferences (visual representation of nudges, e.g. text, progress bar, radio buttons, social influence) will gradually transform their behaviour of using IoT devices. Users will get used to certain recommended practices over time and adopt an accurate user discretion process for privacy choice. Moreover, the consent engine flags possible privacy vulnerability alerts with the occurrence of unintended movements, activation of devices, and enablement of permission within the SB premises.

4.5. Informed Consent Management Engine (ICME)

Prototyping is utilized to assess the feasibility of the ICM and to verify that it will function as envisioned. A reference architecture for the proposed approach is presented, along with an explanation of how the functionalities of ICME support the key characteristics of SBs. A proof-of-concept prototype implementation is presented in Section 5.

4.5.1. ICME Reference Architecture

Fig. 4 presents the ICME reference architecture and shows the key data flows between the different components. A key feature of this architecture is that it redefines the formal structure of the data flows through an IoT network to assess the compliance of data capture and use with the individual privacy policy statements attached to the smart devices.

The privacy policies for each IoT device in the shared smart space (corresponding to *Phase 1* in Section 4.4), the list of predefined permissions *(Phase 2)*, the events associated with privacy breaches or potential risks *(Phase 4)*, and the nudge details *(Phase 5)* are stored in the document database (5). A user can interact with the IoT Device (10) in three different ways; via a mobile application (1), via the IoT dashboard (2) and by using a voice assistant (8). These act as consumers of the ICME API deployed on the ICM Cloud-API server (4). If we consider the scenario of the user interacting with an IoT device via his/her mobile application, then the following data flow occurs. The

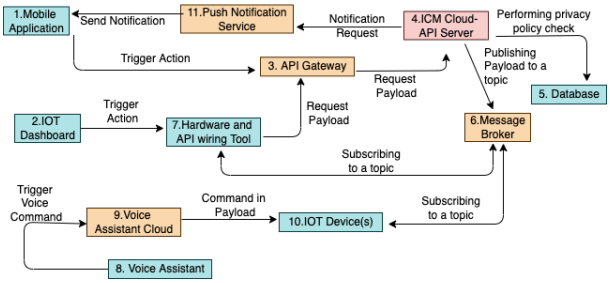

Figure 4: Reference architecture of ICME (The data flow diagram [59])

user request from the application (1) is forwarded to the ICM Cloud-API server (4) via the API Gateway (3) by making Rest API calls. On the ICM Cloud-API server, each variable of the request payload is assessed against the privacy policies in the PDD (5) *(Phase 3)*. Simultaneously, the API publishes the request payload to a dedicated topic on the Message Broker (6), which routes it to the appropriate IoT device subscribed to the same topic (10) after identifying the end-point. In the event of a privacy breach or a potential disclosure of high-risk PII, the event is logged in the database *(Phase 4)*. Following this, the ICM API server also sends a nudge recommending corrective actions to the mobile application using the Push Notification Service (11) *(Phase 5)*. Finally, the device's current status is reflected on the IoT dashboard (2) by forwarding the message via a hardware and API writing tool (7).

Our proposed informed consent engine can be introduced to the standard IoT data lifecycle as a new feature for controlling information flow among multiple devices and users over a cloud server. To achieve this, we employ several tools (firmware and software code), plugins (message brokers) services (push notification, API Gateway), and associated interfaces/applications to apply this privacy-enhancing solution to a real Smart Building setting. The primary benefit of this reference architecture is to provide software architects of IoT with a structured way to enforce this approach to privacy-protected SB infrastructures for their end-users while maximising occupant data safety. Furthermore, based on the capability and accessibility to employ different servers, plugins and tools, there can be many implementations for this generalised reference architecture.

4.5.2. ICME Functions to Support Key SB Requirements

Examples of supporting functions that enable ICME to manage the heterogeneity of SBs, including the features used in our prototype to illustrate the concepts, are presented.

- *Multi-user, multi-device support:* In smart shared spaces, IoT devices are shared by multiple users, each with its own data privacy preferences. To deliver the required service and control for each device's access, we require many-to-many relationships between users and smart devices. Even in a simple smart shared area where personal devices are installed in dedicated rooms for the owner's use - such as a camera, smart light, and door lock - we can observe a complex user-device relationship.

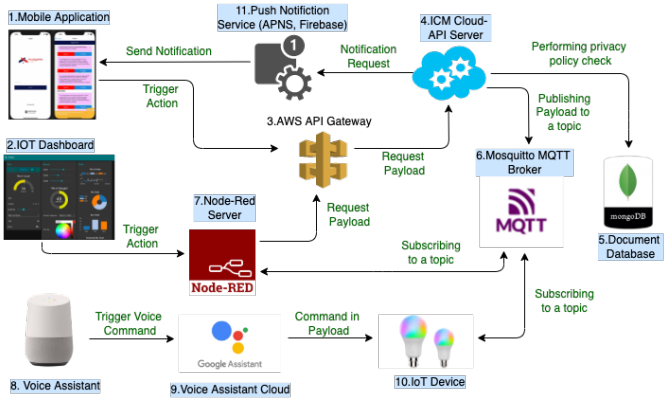

Figure 5: Implemented solution overview of ICME

- *Hierarchical collections of users and locations:* SB solutions need to accommodate different organisational and structural setups. For example, nudges may need to be customised according to the role of an individual within an organisation (e.g., department head, division head, employee, non-staff, etc.). Based on different authority levels, nudges are generated to monitor and control IoT devices' privacy settings within a given *Organisational hierarchy* (i.e. Company > Division > Department > Employee) From this approach, heads of divisions and departments can see the percentage of employees working under him exposed to privacy threats and who needs to further respond to the nudges. Also, the smart building manager can understand how data privacy is managed in his building by looking at the statistics provided by the consent engine. When employees continuously transfer PII data to cloud servers due to unawareness, or any user request contains an unauthorised PII, it will be reflected on the system as a whole. This approach would help the owner identify the loopholes within their IoT network and address them as appropriate. Similarly, there can be multiple individuals and shared rooms, zones of such rooms, floors of such zones, smart sites, or buildings (e.g. Smart office space). Hence, based on the location hierarchy, we customise the output through *Building structural hierarchy* (i.e., Location > Site > Building > Floor > Zone > Room) This provides maximum privacy equally for personal and shared devices.

5. Prototype Implementation

This section presents a specific implementation of our ICME reference architecture.

5.1. Solution Overview

Fig. 5 shows one specific implementation for the reference architecture shown in Fig. 4. IoT deployments in SBs consist of many IoT devices, and it is essential to track, monitor, and manage all the connected devices in a SB via cloud servers. These cloud servers manage the remote IoT device life cycle while playing a crucial role in operating smart devices at scale. With the use of cloud databases and visual programming tools, we designed the ICME prototype as follows.

We used Node-RED[1] to implement a Smart Building IoT Dashboard (2) and for wiring together the hardware interfaces and the ICM APIs (7). Similarly, we used the AWS API Gateway[2] (3) to act as the "front door" for our ICM Cloud API, which was deployed on an Amazon EC2 server (4). The privacy policy database was implemented using MongoDB[3] (5), and MQTT[4] was used as the Message Broker (6). While ICM API acts as a publisher to a specific topic on the Mosquitto MQTT broker(6), which runs on our dedicated Amazon cloud server(4), IoT device(10) acts as a subscriber for that same topic to trigger the action as device's primary functionality. To perform the policy check as the secondary functionality, we capture the request payload (part of transmitted data that is the actual intended message) going through the device manufacturer's cloud platform. These payloads may include user location, availability, calendar data or any other PII (Personally identifiable information). For the purposes of our SB prototype demonstration, "mock-up" interfaces are created for different IoT devices, including Smart Door Lock, Smart TV, Smart Light Switch and Smart Thermostat, that mimic their behaviours (10). Finally, privacy nudges are transmitted to the user via Firebase[5] push notification service (11) and displayed on a prototype iOS mobile application. The code for ICME is available on Github[6].

5.2. *Prototype API development*

We developed the prototype using Typescript 3.8.3 language and NodeJS v14.3.0 as the application server. We integrated Cloud MongoDB as our Document database and used Mongoose[7] as an object modelling tool to create DB models for querying purposes. We chose Amazon Web Services (AWS) as our infrastructure to deploy all API functions using AWS lambda service. We exposed authorised accessibility to our written APIs via an AWS API gateway for consumers (connected through a mobile app/ IoT automation Tool/ Voice Assistant or a collaboration platform for API development, e.g. Postman). All API calls use a Rest API. For testing, we used Postman[8] tool to make Rest API calls that include payload data in the body of the user request. The Rest API calls are intended to send a request to get work done remotely or solicit a response. This creates a test environment to simulate a wide range of example user IoT device interaction requests, IoT device communications, and ICM API calls. The constraints defined in our APIs check if an incoming smart device payload request matches a definition, and will reject it if it doesn't satisfy the requirements.

We prototyped three APIs to (a) perform policy checks and trigger events of IoT devices, (b) generate distinct nudges, and (c) record user privacy permission changes. A Document database collection is maintained to store records of users, devices, and IoT events. Additionally, it contains privacy policy statements attached to each event, personally identifiable information (PII) types with their corresponding sensitivity levels, and lists of authorized devices for each individual and user group based on the hierarchical organizational structure. These collections are joined logically to query/filter records based on smart device payload data. For instance, according to the device token, IoT device ID and event ID, we query an array of applicable privacy policies. Then, we compare all the end-user data objects one by one defined in these policy statements (see Fig. 3) with the variables attached to the payload data. Once this policy check is performed via an API call, it sends an output listing all the privacy policies and end-user data as JSON objects that have been infringed with the execution of user requests. These privacy infringement details are recorded in the database (log history collection) and used to generate distinct nudge content.

We defined a set of privacy nudges to deliver to the user to help improve their smart building device data privacy awareness. Once a nudge is sent to the user, they can act upon it by declining the recommendation or changing their privacy settings. If the nudges have been repeatedly declined in previous attempts, we calculate the frequency of repetitive privacy violations/risks sent to the user when generating different types of nudges. The compulsion of the nudge content is directly proportional to the frequency of such declined similar violations/potential risks. The code for the APIs mentioned above is available in our GitHub repository.

5.3. *Deployment of Prototype Components to AWS*

After deploying the ICM APIs on an AWS instance, an AWS API Gateway and lambda functions are created in the AWS cloud services. Our deployed ICM APIs act as publishers to pre-defined topics in the MQTT message broker on AWS. Finally, the AWS IoT core[9] is configured with special instructions to be used with Node-RED MQTT nodes.

5.4. *Design data flows for a smart lab*

For our ICME prototype implementation, we simulated the setup of the HumaniSE lab[10] as a smart building environment. As shown in Fig. 7, the lab includes private rooms, meeting rooms, open-plan working spaces and shared areas. For a SB demonstration, we have configured the lab with seven smart light interfaces, four smart door lock interfaces, two smart TV interfaces, and five smart temperature sensor interfaces. Node-RED is used to implement smart space automation operations by wiring together these different devices, the ICM APIs and the Nudge Notification Service.

The data flow design is different for each type of smart device. Fig. 6 shows data flows that are numbered and partitioned

[1] https://nodered.org/
[2] https://aws.amazon.com/api-gateway/
[3] https://www.mongodb.com/cloud
[4] https://mqtt.org/
[5] https://firebase.google.com/
[6] https://github.com/chehara/ICM_repo
[7] https://mongoosejs.com/
[8] https://www.postman.com/
[9] https://aws.amazon.com/iot-core/
[10] https://www.monash.edu/it/humanise-lab/home

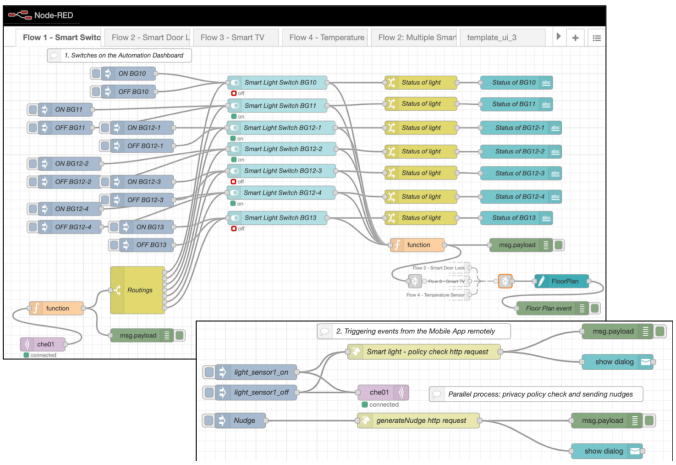

Figure 6: Data flow definition for smart lights in the HumaniSE Lab - Node-Red admin user interface.

Figure 7: Node-Red Dashboard for the HumaniSe Lab (with floor map integration)

into multiple tabs on the same canvas for convenience. For example, the first tab in Fig. 6 shows the data flow definition for the smart lights in the HumaniSE Lab. We can define such data flows for any type of smart space setup, including hierarchical ones as discussed in Section 4.5.2. As this implementation consists of multiple link nodes and sub-flows, we can easily reuse existing nodes while affording any demanded scalability. This data flow design is a reusable artifact that can be used for any future application for any smart office setting and is one of the key contributions of this study.

5.5. Dashboard for the Smart Space

An IoT dashboard is a key human-machine interface that organises and represents a digitalisation of the physical world in a single interface that can access and control a given environment from anywhere in the world. We have used Node-RED to implement our SB dashboard, which provides users with a real-time view of each smart space and its different IoT devices in the shared space. As shown in Fig. 7, the dashboard layout is laid out as a grid. It consists of multiple dashboard nodes (e.g., charts, gauges) to express the live status of each device. Based on the number of buildings, rooms, floors, and divisions in our smart space, the design can be customised to position all the smart devices installed in a real environment. Fig. 7 demonstrates the dashboard in use for our HumaniSE lab smart space with the floor map integration. Users can see the current status of each smart device and check if it is functioning according to the constraints defined in the data flow. The ICM API calls are executed in parallel to perform policy checks and generate user nudges.

5.6. ICME Digital Nudging Examples

Digital nudging is used for positive reinforcement, highlighting what privacy settings should be practised by the SB inhabitants to secure and protect their PII. As illustrated in Fig. 8, we have provided an option for the user to react to or decline a pop-up message generated for each type of nudge. Different types of nudges are delivered to the user based on the declined nudge frequency calculation (as described in Section 5.2). Also, each nudge includes a "Tell me more..." feature to debrief the calculation and examine the history of events. All generated nudges with the user action are recorded in the database to measure nudge effectiveness against user behaviour change in the future. Below, we list nine different nudge types, based on existing literature on nudging and human decision-making ((see 2.4) that have been implemented in our prototype.

- *Type 1: Awareness.* This nudge type seeks to raise users' privacy awareness to protect them from possible privacy infringements. e.g. *Your <PII Type> has been shared <n> times during the last <x> days.*
- *Type 2: Awareness and Control.* In addition to informing the user of possible privacy infringements in recent data transmissions, Type 2 nudge includes a control condition statement to guide users in addressing the situation. e.g. *<Type1 awareness statement>, Consider changing privacy settings.*
- *Type 3: Awareness and Coping Appraisal.* In coping appraisal, people assess *response efficacy*, i.e., whether undertaking a recommended course of action will remove the threat, and *self-efficacy* i.e., their level of confidence in being able to carry it out. Type 3 nudges include a coping appraisal statement and the awareness statement. e.g. *<Type1 awareness statement>, You can easily minimize the possibility of suffering privacy breaches, if you disable <service name> sharing services.*
- *Type 4: Awareness and Threat Appraisal.* In threat appraisal, people consider the *perceived severity*, i.e., how negative the threat's consequences, and *perceived vulnerability*, i.e., likelihood of the threat materialising. Type 4 nudges include threat appraisal and threat awareness statements. e.g. *<Type1 awareness statement>. If you do not disable your <PII Type> sharing privacy settings, your personal data could be compromised and you can be tracked or profiled.*
- *Type 5: Awareness and Herd Behaviour.* In addition to the awareness statement, we included figures on popularity to inform how others have restricted information disclosure(Social nudge). e.g. *<Type1 awareness statement>.*

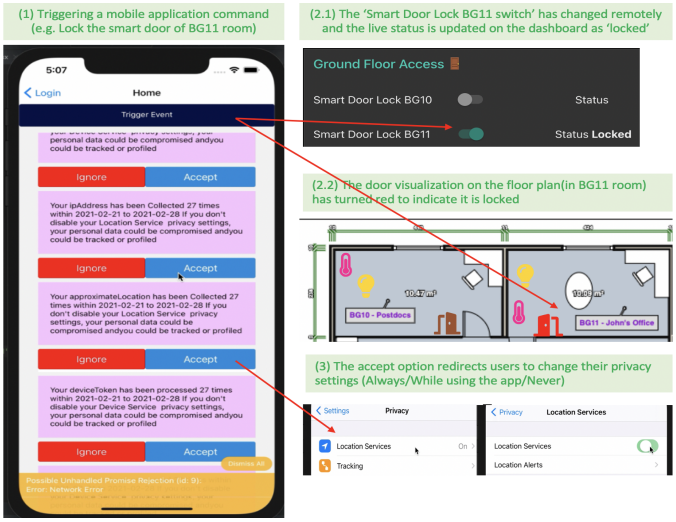

Figure 8: Nudge visualisation respect to the end user data objects of Fig. 3, controlling of devices and their privacy settings via mobile app

<Percentage> of your colleagues do not share <PII Type> with others.

- *Type 6: Coping and Threat Appraisal.* In this type, we combined the Type 3 nudge with the Type 4 nudge.
- *Type 7: Male or Female Anthropomorphic character.* Anthropomorphic characters are male or female human-like images that appear with the nudge content to increase user's trust. Furthermore, previous empirical findings on nudges to security behaviour have proven that a male anthropomorphic character increases security behaviour. e.g. A quote by a male or a female with an image.
- *Type 8: Awareness and Gain.* This type of nudge highlights what users can obtain if they proceed with the privacy setting changes. e.g. *<Type1 awareness statement>. By changing your privacy settings, you could protect your personal data from prying smart <Device name>.*
- *Type 9: Awareness and Loss.* This type of nudge highlights what users will lose if they do not proceed with the privacy setting changes. e.g. *<Type1 awareness statement>. If you do not change your privacy settings, you could lose your privacy in protecting your data.*

5.7. Mobile App development and Nudge Visualisation

We prototyped a mobile application for interacting with the ICME smart space devices and to visualise and respond to digital nudges about privacy threats and settings. The application displays the recent nudges received by the user, categorised under each smart device and its action (e.g. Smart TV - Process action). Fig. 8 illustrates how the Type 4 nudge is activated. When a user triggers an event (1) to lock the Smart Door via his mobile application, the request is processed by the ICM APIs. The dashboard reflects the device's live status using different colour codes and visual indicators (2.1, 2.2). The smart door lock trigger command is connected to his phone and can access his location data through the mobile phone's location service technology. The repeated approximate location access raises a data privacy reminder and the smart lock device's PII accessing behaviour is visualised as a nudge on the app. Finally, the user can respond to the nudge and change the privacy settings (3).

6. Evaluation

We have qualitatively evaluated the ICME approach and prototype using expert interviews. Below, we provide details of how this evaluation was carried out.

6.1. Ethics Approval

Ethics approval was obtained from Monash University's Human Research Ethics Committee (MUHREC) prior to conducting the expert interviews (a low-risk research project approved on July 2, 2021). All documents relevant to the data collection process, including the explanatory statement, consent form, recruitment email, advertisement, and interview protocol, are included in Section 7.

6.2. Planning Interviews

We used a seven-stage process to conduct the study [60] – (i) *thematise:* define the purpose of the investigation and present how the theme can be investigated; (ii) *study design:* collect generated knowledge from the participants and consider the ethical implications of the study; (iii) *interview:* use an interview guide with a reflective approach to the knowledge we seek and the interpersonal relations of the interview situation; (iv) *transcribe:* the interviews to text and anonymise details of the people, locations, and events which are mentioned in the interview; (v) *analyse:* we consider the nature of the interview material, which modes of analysis are appropriate for the interviews – we applied a six-phased reflexive thematic analysis [61]; (vi) *verify:* we ascertain the interview findings' validity, reliability, and generalisability; (vii) *report* the findings.

6.3. Data Collection

Interview Protocol: We conducted an interview study to collect qualitative, open-ended data to explore participant thoughts, feelings and beliefs about ICME and privacy in IoT-oriented SBs. We formulated a set of semi-structured questions [62], e.g., *"Can you recall any framework or model that caters the informed consent management in SB Environments"*. The participants shared examples of projects and measures they experienced or applied previously to address privacy concerns. We followed up by asking more concrete questions such as *"How did you determine the <participant defined example> would best fit with the <participant defined project> ?"*. We conducted a pilot study involving two participants (researchers working for Monash smart cities) known to the first author, and not related to the research, to ensure that the questions conveyed the expected meaning. The questionnaire was fine-tuned based on the feedback received from these two baseline respondents.

Participants: A total of 15 experts (13 male and 2 female) from the industry and academia belonging to two distinct groups (Security and Privacy Experts, and SB and IoT infrastructure designers) were recruited for our evaluation. Recruitment was carried out by (i) directly contacting suitable candidates that were known to the investigators' via personal email

invitations or (ii) contacting those who expressed interest in a LinkedIn advertisement about the study. Email invitations were sent to the selected candidates following a rigorous screening of their profiles. The participants' years of relevant experience varied from *8 to over 25 years*; more than half of them had over 15 years of industry experience. The participants were from Australia, New Zealand, Brazil and Sri Lanka. However, their career experience spans beyond their current locations and includes Germany, the Middle East, India, Egypt, Sweden and the United Kingdom. There were eight participants from the industry and four from academia with expertise in Security and privacy specialists (knowledgeable in IoT). Similarly, there were two participants from the industry and one from the academia with expertise in SB and IoT infrastructure designers (knowledgeable in privacy).

Conducting the Interviews: Prior to the interview, all participants were provided with a short video[11] highlighting the primary research problem, the research objectives, a brief overview of the proposed approach, and a demonstration of how it works using the following scenario:

"Johnny, a member of the HumaniSE lab[12], prefers to turn on his smart heater and the lights on his way to his room using an office automation mobile app, which continuously captures his current location. Once he enters the room, he checks his daily calendar schedule and sets his smart door lock to be locked/unlocked automatically. After several months he notices that he is receiving some strange personalised emails and advertisements from unauthorised third parties. He is now annoyed due to the disclosure of his personal data via smart devices, including his calendar and location details, without being aware of the consent and privacy policies. After reporting this incident to the management, they decide to integrate ICME into their Building Automation System (BAS) to better control IoT devices' privacy. Johnny can now interact with the IoT devices of any smart space in three different ways; via a mobile application, an IoT dashboard, and a voice assistant. These are consumers of the ICME API, deployed on the Amazon Cloud-API server, which performs policy checks. When Johnny interacts with a device via his mobile app, the API captures the associated event payload to assess the event-specific policy statements stored in the MongoDB document database. All the applicable policies are tested and the results are logged as true or false to indicate any policy infringements and potential disclosure of high-risk PII. If any privacy issues arise, the API nudges Johnny and recommends corrective actions to his mobile application. Simultaneously, a message broker routes the request to the appropriate device."

The semi-structured interviews were conducted remotely via Zoom primarily due to the COVID-19 pandemic and also because several participants were located overseas.

6.4. Data analysis

The 15 interviews were recorded and transcribed using Otter.ai[13] and then manually verified. We performed a reflexive Thematic Analysis (TA) on the descriptive answers received for the interview questions. TA is a method for "identifying, analysing and reporting patterns (themes) within data" [61]. The demonstration and questions for evaluating our proposed approach are based on some pre-defined concepts intended to be covered through the interview study (e.g., use of digital nudging, interoperability of the solution, issues in getting informed consent from IoT users, and beneficiaries of ICME). We used NVivo software[14] to organize the textual data and create graphical displays. This assisted in discovering patterns of codes and links between codes across large fields of data.

6.5. Results

The key findings from our evaluation study are demonstrated in two aspects: (a) the inherent complexities relating to data privacy for various IoT implementations (based on the experts' experiences with similar use cases in their professional careers), and (b) the timeliness of the proposed model and reference architecture for managing user consent in SBs. We assign an identification code to denote each participant as IV(n); n = 1,2,...,15.

6.5.1. Data privacy complexities

The majority of the experts noted the originality of our proposed solution to enhance the visibility of IoT data capture and circulation across cloud platforms and beyond, e.g. *"once you disclose your sensitive data to the cloud, it's gone. Therefore, it's better to take precautions to decide what to release and what not to release as recommended by the ICME"* [IV9].

The experts concurred that people always tick the "terms and conditions" box to quickly consume the service or the product features. By ticking the box, users agree to a vendor's privacy policy. However, a policy merely tells users how the service/product provider will handle user information, and is not a request for consent. Therefore, ticking the box cannot be considered valid consent but merely a term of entry [IV15]. Respondents also noted that when users purchase a smart device, they always have to give consent to continue with the subsequent processes [IV4]. The decision is Boolean; either accept or reject without any flexibility [IV6]. Experts highlighted this as one of the weaker privacy controls in IoT systems.

More precisely, *"Smart peripherals collect data as per the user agreements, but how they handle that information is still a grey area. A recommendation offered by such devices is highly unlikely to be a part of the privacy legislation/policy/guidelines ... there may be organisations that have adopted cybersecurity frameworks (e.g. NIST) and Privacy Acts (e.g. GDPR) for their IoT development. However, these terms are not specific or relevant to a product despite providing a comprehensive and applicable holistic view"* [IV14].

According to the literature, some products may comply with all the relevant privacy terms and conditions; they can be adequately deployed, but privacy can never be ensured due to unforeseen privacy risks. One interviewee highlighted that the return we get depends on how much data we are willing to trade

[11] https://youtu.be/5y6CdyWAdgY
[12] https://www.monash.edu/it/humanise-lab/home
[13] https://otter.ai/
[14] https://www.qsrinternational.com/nvivo-qualitative-data-analysis-software/home

off. For instance, *IoT companies collect the data and may try to sell or make profits from it, and later we are potentially paying double or triple the price for this compound picture* [IV4]. These privacy implications are compounded when users cannot control the devices with reasonable visibility. For example, *sensors are trickier to be controlled as they operate in the background with limited interactions and human interfaces except for blinking lights* [IV12].

From the experts' point of view, multiple people will review the same codebase and design within any IoT organisation to ensure quality and privacy. Nevertheless, they belong to the same building/office space, and probably they could be serving as colleagues or mentors who teach new staff. Thus, it was noted that there is a high probability of making the same mistake [IV4]. Therefore, privacy controls are weaker across IoT, though it has been around for a long time. There are still many privacy gaps in IoT, although organisations and researchers are making efforts to improve it. Some examples from expert observations include: IoT vendors and companies are concerned about being *'caught in the crossfire' of negative publicity or scrutiny* from a regulator. While they may not be interested in serving the community or doing the right thing, they definitely take action if they are hit with regulatory fines or community complaints. *Thus, recently we can see more privacy by design at the early manufacturing stage* [IV15].

6.5.2. Timeliness of the ICME approach

Experts noted that there are a variety of different consent management platforms, models, tools and frameworks for web systems, browsers and apps [IV2, IV5, IV12]. For example, besides the default mode, social media platforms such as Twitter or Facebook also support sophisticated privacy settings. Similarly, some systems allow novice users to follow the behaviour of security and privacy experts by choosing the settings chosen by them [IV1]. Digi me[15] is a consent service where a person can handle all their consent contracts for various information uses across platforms through one channel [IV15]. It sends a request to the applicable User Storage to release the *ReleasedData* to the Developer Application. Some intelligent Data Analytics and Machine Learning tools can automatically analyse the data and reveal particular combinations of attributes or values that are at significant risk of privacy leakage, as the number of records satisfying that specific combination of attribute values is overly low. If an attacker could come up with such a combination of attributes, they can reveal sensitive patterns, and reveal PII [IV9]. Therefore, these intelligent tools, frameworks and models can assist or warn users and developers to preserve data privacy (e.g. by limiting data collection) to a certain extent while enhancing user awareness.

However, the experts stated that there are several limitations and difficulties in using existing tools or inventing comprehensive frameworks. For instance, employees do not always get to decide the tools/automated solution required to protect IoT-oriented systems from unintended privacy implications as organisations need to maintain a delicate balance between being up-to-date and being cost-effective [IV2]. Also, most of these tools are partly automated as there are many intelligent and privacy-preserving processes that cannot be easily transformed into automated processes to manage user consent and validate controls. Many tools, including Governance, Risk and Compliance (GRC) tools such as Archer, Camms, or MetricStream can capture this information. Yet, *there is a need to aggregate and cast human eyes over it in meeting sufficient compliance levels* [IV2]. Manual checking is still required as the tools can only support a certain amount of automation for IoT organisations.

All the interview participants agreed that they have previously not seen a consent management solution such as ICME. In most cases, they said that privacy laws do not require consent. Instead, they require notice, and consent applies if we decide to do something unintended with user information or give it to a third party in a different circumstance. *Informed consent usually comes after we already have the information and we are going to use or disclose the information in a way that the person does not understand or does not expect* [IV15]. In addition, the experts stated that it would be *beneficial if the user knows when and how much data or preferences from the smart devices that are linked back to the users were going out to the Cloud; they know when it is not what the user signed up for and the terms and conditions; if they had an opportunity to vary their consent; change the understanding of what they are trading off* [IV8, IV15]. The participants shared a common view that the technical aspect of improving privacy for IoT is still evolving. In contrast, *the human factor plays a vital role in making educated decisions that the community does not understand well with the given information* [IV4]. Therefore, terms and conditions are outdated ways of making people aware of agreements, and this is where the ICME concept comes timely in the initial smart device infrastructure design stage and beyond.

It was noted about the ICME approach: *"This is an excellent idea . . . Some popular reference architecture already exists for smarter environments, such as Cisco, IBM or Intel reference architecture for IoT . . . However, . . . it doesn't have anything related to privacy. So if we can develop this reference architecture with privacy as an additional layer, it will be amazing. The currently applied standard is only an engineering architecture without integration of engineering with privacy in one place - because it does not exist [IV7]."*

6.5.3. Strengths of ICME

S1: Supports software developers in developing enhanced privacy and consent management solutions for smart spaces: The experts stated that most developers find it challenging to design, develop and deliver novel privacy solutions for IoT. *"Absolutely, it supports both novice and expert developers"[IV2, IV15] and is beneficial for consumer advocates for companies in obtaining great benefits" [IV3].*

Instantiating a fully functional reference architecture that caters to the emerging requirements of the IoT domain requires further research and domain area expertise. With ICME, the top-level management or strategists can configure each role within the organization properly, without relying on the developer, and ensure that the outputs go through the ICME

[15] https://digi.me/partner-terms/

engine to ensure privacy enforcement [IV10, IV11]. ICME raises awareness as a lot of developers involved in mobile or IoT applications use third-party components and SDK libraries. They do not know the extent of data that these libraries are sharing. Often, the SDKs are used for convenience, but the providers of such libraries may want them to be consumed as a source of income or for advertising. In some instances, the developers are liable for sensitive data breaches instead of these third-party library providers [IV12]. Therefore, developer experience also matters in some specific use cases. The success of the ICME platform would depend on how easy it is for developers or companies to use it while delivering services to the end user [IV10]. Therefore, experts stressed that it is always valuable to have a reference architecture rather than reinventing the wheel. With ICME, any organisation that wants to develop a consent management solution has a solid framework and prototype to start with [IV12, IV10] although new requirements may emerge around system integration and configuration, and with security add-ons [IV14].

S2: Supports platform independent implementation: The experts acknowledged that the ICME architecture and the prototype can solve a massive problem as its simplicity by design would convenience embedding privacy within existing solutions. Any IoT service provider or vendor can use it if they meet all the clearly defined rigorous guidelines [IV10]. In addition, the experts highlighted that they had not previously designed the reference architecture for a particular service platform as the implementation is independent of any substituting service/platform/tool [IV15].

S3: Improves user awareness and visibility to data by making information more useful: With the rapid adoption of IoT, every home/apartment has at least 10-15 smart devices. Users are supposed to be fully aware of what applications are requesting personal data and what the application does with their request permissions. Based on the experts' opinion, buying secure products from quality vendors than relying on cheaper devices or having a good firewall would limit this collection and misuse of data. However, not everybody has the knowledge or capability to be privacy-aware at an advanced level around their smart devices, so it is timely to have a tool/reference architecture to ensure data privacy across cloud platforms [IV3, IV4].

By providing more context around the data being collected, ICME helps users make better, more-informed privacy decisions. Experts also highlighted that as a result of leaving the Wi-Fi modules switched on all the time, a user's MAC address can be collected using rouge Wi-Fi access points and used to draw a trajectory of a user's commute route [IV9]. Therefore, experts acknowledged that our solution is practical to make people aware of potentially sensitive data leakages [IV3, IV9] as IoT device applications may often access user data [IV6]. For instance, ICME uses nudges to address one of the complex challenges in privacy, i.e., to positively change users' privacy decisions [IV1, IV6].

S4: Supports personalised privacy decision-making experience. *"I have 34-38 mobile devices at home, including my children's, and if I can get a snapshot of all the devices and how the captured data goes beyond the user consent or privacy policies, I would love to know what kind of dashboard I get [IV3]"*. With Node-Red integration, ICME provides a personalised privacy dashboard for users with live status display for all their IoT devices. In addition, experts mentioned that it can capture the data and visualise the privacy information while delivering significant insights to its owner [IV12, IV10]. Given privacy dashboards, users can start comparing solutions from diverse vendors and assess which providers share excessive amounts of data and which providers are more likely to share a reasonable amount of data, leading to increased awareness about the data collection practices of different vendors [IV12].

S5: Encourages accountability among service providers: ICME architecture and prototype help to build trust and transparency over data when an owner of a SB is not trusting the infrastructure itself and prefers to see what is happening with the internal data captured from their smart devices [IV6]. It puts individuals in control of their privacy while holding the service-providing organisations to a higher degree of accountability. Therefore, experts pointed out that organisations must be honest and have up-to-date privacy policies to maintain users' trust in their devices. Also, what they initially state as the utility of their personal information should be all they do with it [IV15]. Furthermore, the manufacturers developing IoT devices can benefit from building better security and privacy controls upfront with the new legislation changes in enforcing better privacy at design and manufacturing time [IV2].

S6: Outbound traffic testing component for vendors: One of the participants suggested that the ICME framework can be transformed into a testing component for IoT vendors to ensure they are not inappropriately sharing consumer information [IV15]. The "ICME Cloud API server" can be used to test the outbound traffic can be tested during product development. Using it, developers can build compliance-driven IoT products and sensors if they can parse the test payloads across the ICME API to verify the data variables against user consent. In addition, some companies have their own privacy dashboards that only work with a specific product line. ICME can remove this interoperability issue by becoming a proxy in the middle, amending the media or capturing the traffic and giving them required privacy information [IV12].

6.5.4. Limitations of ICME

Some of the limitations identified by the experts are discussed below. While some of them are at a conceptual level, others are either functional or empirical and will likely become apparent when the system is deployed at scale.

L1: Inconvenience of nudges. According to the experts, as the number of connected devices in a smart space increases, so does the number of nudges received by the users [IV7]. Many users tend to turn off the notifications if the nudging frequency is too high [IV6, IV7]. Moreover, they may hesitate to engage with the nudges if they find it challenging to digest the level of information provided [IV13]. Therefore, it is important not to overload the user with information. A potential solution is to experiment with each type of nudge to discover which one works the best for a given user [IV12].

L2: Building trust in ICME: *"With the integration of our work . . . people may ask . . . how can they trust the ICME framework provider instead of the IoT device manufacturer as they can be tech giants in the market for years" [IV5].* This concern might be an issue for any stakeholder who does not trust the third party completely [IV6]. Therefore, we should be able to convince the potential stakeholders of ICME (e.g. IoT vendors, SB owners, OS providers) by clarifying the transparency of our operations, authenticity in its behaviour, and reliability in its performance. This approach will gradually build stakeholder trust and positively influence data privacy.

L3: Using IoT services instead of actual devices: The experts held the view that there is a significant difference between a physical IoT device and a service. While the IoT service mimics the functionality of transmitting a payload, the physical device gets authenticated to the environment and performs underlying device-cloud communication to operate as triggered [IV7]. Experts further highlighted that as we are replicating the IoT infrastructure to support compliance checking, we have full control over data and requests, which might be restricted or filtered in real environments [IV4]. In addition, there are device drivers based on the profile of the device (e.g. device name, device firmware, device location) and this information can only be fetched from a real device [IV7].

L4: Interoperability issues across multiple communication standards: The ICME reference architecture can be implemented with compatible tools/servers/database settings. As explained in Section 5.1, we used the MQTT IoT protocol for service integration, and it has a solid abstraction layer to perform all the transactions across the cloud securely. To support an increasing number of message brokers to foster the concept of webhooks, we should have the ability to integrate across multiple communication standards. For instance, there are many other frameworks used by organisations such as CoAP, AMQP and DDS, in addition to the widely used REST API calls over MQTT [IV10]. Currently, we have not tested all the possible permutations with the popular IoT protocols, but we believe that ICME can be integrated with any compatible protocol. Moreover, interoperability becomes more challenging as we extract privacy policy statements from many linked documents from diverse IoT vendors. Therefore, many software systems practices followed by IoT vendors will have to become adequate and comprehensive for our work to proceed [IV12].

L5: Granularity of the consent mechanism: A key challenge in designing ICME was supporting granularity over the initial and ongoing consent mechanism considering different levels of data sensitivity [63]. There were implementation limitations to defining consent under dynamic conditions. E.g., granting access to sensitive data in case of emergency or during a certain period of time; but at other times, blocking access by a third party [IV4] [64]. In addition, when using IoT devices, users may have two extremes: provide consent in all cases to consume the service straightaway or without giving consent to a rigorous policy yet consume the service [IV6]. However, users cannot customise their consent with the standard IoT setup. Therefore, the level of granularity expected from ICME varies with the data subject (e.g., age, gender, computer literacy, medical condition, privacy awareness) and their preferences against privacy decisions.

6.6. Threats to Validity

Below, we discuss some of the threats to the validity of our study. They are categorised into three groups as follows:

External: Due to unreachable access permissions to third-party cloud servers, the complexity of the development, and the associated high costs, we had to make several assumptions and design decisions for our prototype. They are as follows: (i) IoT device interfaces have been used to react and respond similarly to the physical device, (ii) even though IoT devices can be controlled in three different ways, we demonstrated only two options (mobile application and IoT dashboard) , (iii) we decided to work on a private cloud server from the very beginning and did not consider the interoperability issues when working across multiple vendor clouds (configurations, authentications, complex customisation), and lastly, (iv) a large-scale community field study to measure the improvement in awareness among the users is not possible since we are currently not using any commercial IoT devices for the prototyping.

Construct: Our prototype supports the manual extraction of privacy policies associated with IoT devices. Such extraction must be monitored and reviewed by a domain expert. Also, our solution cannot detect deception in IoT devices when personal data is obtained by intentionally misleading the subjects and used for unspecified purposes (e.g. when data variables are defined in the policies without full disclosure).

Internal: In terms of the interview study, most of the experts were from Australasia, but their years of experience span four continents, limiting the biases. In addition, we reached theoretical saturation in the qualitative analysis at 12 participants (e.g. gradual decrease of emerging new patterns and no significant themes or codes emerging from data). To confirm it we conducted three additional interviews.

6.7. Future work

The following recommendations are listed based on the analysis of the interview results, our findings from the literature, and the insights gained from modelling and prototyping.

R1: Use machine learning to automate code reviews, policy extraction and context-driven consent management: Privacy-preserving ML can be applied to limit the potential risks to sensitive data. E.g., most privacy-preserving ML techniques use differential privacy that focuses on the posterior probability making every possible likelihood (probability) look the same [IV9]. Similarly, experts mentioned that NLP techniques can be used to analyse the code to find potential privacy breaches that cannot be detected by existing techniques. This reduces human errors when reviewing peer codebase [IV4].

R2: Keep data closer to the user's trusted zone: The data collected at a macro level should not be moved out of the trusted zone. E.g., experts highlighted that data must stay within the smart office or home network without flowing into a third-party provider's storage facility. Keeping data within boundaries is essential in corporate sectors, including healthcare and defence, as SB data aggregation goes beyond one service provider [IV5].

R3: Design better nudge visualisations to help users understand the potential privacy leakages: Based on expert opinion, it is often challenging to design nudges expressing privacy risks that are easily understandable. It requires an extensive user study to learn what language people understand to influence their privacy decisions positively [IV1]. Simple language and graphical control elements (e.g., progress bar, toggle buttons, warning colouration, etc.) could be used that anyone can understand in layman's terms [IV6]. For example, presenting limited options and representing the risk levels on a bar may help end-users understand how privacy could be preserved by modifying their decisions [IV6, IV9].

R4: Include device specific privacy variables in addition to PII: While PII is directly related to individuals and can lead to their identification, sometimes it is possible to infer personal information from device-specific information as well. Therefore, it is important to consider each IoT device as a separate private entity and extend ICME's PII bank with additional privacy variables [IV7].

R5: Build ICME as a modular, reusable building block for consent management in SBs: Our experts suggested that ICME should be a universal standard building block that supports multiple products, vendors and solutions [IV14, IV12]. "So without making the current market a mess, we can support different collaborations. For example, Google teamed with IKEA products" [IV12].

R6: Use ICME as a security penetration testing tool to discover unknown privacy threats: Experts stressed that developers are not adequately performing basic security testing for their apps. E.g., when using a smart bulb, the application automatically asks permission to capture your location data. Yet, it collects location data until the user turns off the device [IV12]. It would be beneficial to use the "ICME cloud API server" as a testing tool to understand any unspecified capabilities of a given source code and scan huge repositories in providing advice based on unfitting user consent [IV4, IV13]. In addition, experts mentioned that organisations continuously look for easy methods to comply with privacy standards as it is complex to satisfy end-to-end data privacy [IV2].

R7: Use systematic or mathematical models to quantify the privacy level of the smart environment: The risk of smart environments can be quantified by measuring the privacy levels of all the connected devices in it. Based on the experts' opinion, fuzzy logic, fuzzy inference or simple probability calculations are some of the ways for quantifying risk. It is important to keep it simple as people do not look for complicated privacy indexes or instructions [IV7]. In addition, having a heatmap that summarises all the nudge contents would be engaging for users who would prefer to see the privacy implications of all the connected devices in one snapshot [IV6].

7. Conclusion

A key challenge associated with privacy preservation in IoT-enabled Smart Buildings is that the data collected by different IoT devices can be combined to reveal potentially sensitive information about the occupants. Yet, research shows that users typically have no awareness of this, and therefore fail to take the necessary steps to safeguard their privacy. To address this problem, we first enumerated some of the key research requirements for informed consent management in shared smart spaces. Next, based on those requirements, we presented our novel informed consent model(ICM) and consent management engine (ICME), which can be used to implement diverse end-user consent management solutions for a variety of shared smart spaces. ICME offers end-users better visibility and control over the data that is being collected about them and enhances transparency between the service providers (organisations) and the end users(consumers). Then a generalised reference architecture is introduced for ICME followed by a proof of concept implementation for a simulated smart shared workplace to demonstrate practical feasibility. This prototype implementation illustrates how the proposed framework (a) enhances user awareness, (b) helps detect privacy compliance and infringement by IoT devices, and (c) improves users' privacy-protecting behaviours, through digital nudges. Finally, following ethics approval, an expert interview study is conducted with 15 highly experienced industry professionals and academic researchers to validate the proposed approach. Through thematic analysis of the interview transcripts, a total of seven key strengths, seven limitations and fourteen recommendations are identified after merging forty-three codes through three iterations.

Acknowledgments

Pathmabandu was supported by a CSIRO Data61 PhD scholarship. Grundy is supported by ARC Laureate Fellowship FL190100035.

Appendices

Link to interview study documents (explanatory statement, consent form, recruitment email, advertisement, and interview protocol) : https://bit.ly/39g4no1

References

[1] Internet of things (iot) connected devices installed base worldwide from 2015 to 2025, https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/.

[2] N. Saputro, A. Yurekli, K. Akkaya, S. Uluagac, Privacy Preservation for IoT Used in Smart Buildings, 2016, pp. 129–160.

[3] P. K. Venkatesh, D. A. da Costa, Y. Zou, J. W. Ng, A framework to extract personalized behavioural patterns of user's iot devices data, in: Proceedings of the 27th Annual International Conference on Computer Science and Software Engineering, CASCON '17, IBM Corp., USA, 2017.

[4] M. Henze, et al., A comprehensive approach to privacy in the cloud-based internet of things, Future Generation Computer Systems 56.

[5] S. Kokolakis, Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon, Computers & security 64 (2017) 122–134.

[6] K. Renaud, I. Bongiovanni, N. Aleisa, The privacy paradox: we claim we care about our data, so why don't our actions match?, https://bit.ly/3PNkl8F.

[7] J. R. Eiser, C. Eiser, Prediction of environmental change: Wishfulfillment revisited, European Journal of Social Psychology 5.

[8] M. Williams, J. R. C. Nurse, S. Creese, The perfect storm: The privacy paradox and the internet-of-things, in: 2016 11th International Conference on Availability, Reliability and Security (ARES), 2016, pp. 644–652.

[9] P. E. I. Network, General data protection regulation(gdpr), https://gdpr-info.eu/ (2018).

[10] M. Seliem, K. Elgazzar, K. Khalil, Towards privacy preserving iot environments: A survey, Wireless Communications and Mobile Computing 2018 (2018) 15.

[11] R. Clarke, What's' privacy', in: Australian law reform commission workshop, Vol. 28, 2006.

[12] A. H. Maslow, A theory of human motivation, Psychological Review 50 (4) (1943) 370–396.

[13] R. L. Finn, D. Wright, M. Friedewald, Seven types of privacy, in: European Data Protection, 2013.

[14] Attorney-General's, Federal register of legislation - australian government, https://www.legislation.gov.au/Series/C2004A03712.

[15] Hipaa australia: The privacy act 1988 - compliancy group, https://compliancy-group.com/hipaa-australia-the-privacy-act-1988/.

[16] PIPEDA, The personal information protection and electronic documents act (pipeda) - office of the privacy commissioner of canada, https://bit.ly/3Avhq07 (2019).

[17] K. Courtney, Privacy and senior willingness to adopt smart home information technology in residential care facilities, Methods of information in medicine 47 (2008) 76–81.

[18] N. Mohammadi, J. Leicht, L. Goeke, M. Heisel, Assisted generation of privacy policies using textual patterns, 2020, pp. 347–358.

[19] P. G. Kelley, L. Cesca, J. Bresee, L. F. Cranor, Standardizing privacy notices: An online study of the nutrition label approach, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, Association for Computing Machinery, New York, NY, USA, 2010.

[20] K. Ghazinour, T. Albalawi, A usability study on the privacy policy visualization model, 2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing (2016) 578–585.

[21] A. Silva, et al., Improving the specification and analysis of privacy policies - the rslingo4privacy approach, 2016, pp. 336–347.

[22] I. Corp., Ibm p3p policy editor, https://www.w3.org/P3P/imp/IBM/ (2002).

[23] OAIS, Australian privacy principles guidelines, chapter b: Key concepts (2019).

[24] C. Yeginsu, If workers slack off, the wristband will know. - the new york times, https://nyti.ms/3pEas2j (2018).

[25] M. Rhodes, A gadget designed to finally make doctors wash their hands enough | wired, https://bit.ly/3CtDWHY (2014).

[26] K. Berg, T. Spil, R. Effing, The Privacy Paradox of Utilizing the Internet of Things and Wi-Fi Tracking in Smart Cities, 2019, pp. 364–381.

[27] M. Seliem, K. Elgazzar, K. Khalil, Towards privacy preserving iot environments: A survey, Wireless Communications Mobile Computing 2018.

[28] C. Castelluccia, M. Cunche, D. Le Métayer, V. Morel, Enhancing transparency and consent in the iot, in: 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), IEEE, 2018, pp. 116–119.

[29] A.-R. Lee, Investigating the personalization–privacy paradox in internet of things (iot) based on dual-factor theory: Moderating effects of type of iot service and user value, Sustainability 13 (19) (2021) 10679.

[30] N. Aleisa, K. Renaud, I. Bongiovanni, The privacy paradox applies to iot devices too: A saudi arabian study, Computers Security 96.

[31] G. Developers, Appopsmanager | android developers, https://developer.android.com/reference/android/app/AppOpsManager (2014).

[32] NortonLife, App advisor feature in norton mobile security, https://support.norton.com/sp/en/au/home/current/solutions/v97499944 (2020).

[33] R. Mitev, A. Pazii, M. Miettinen, W. E. and, Leakypick: Iot audio spy detector, https://arxiv.org/pdf/2007.00500.pdf (07 2002).

[34] R. van Bavel, N. RodrÃguez-Priego, Nudging online security behaviour with warning messages: Results from an online experiment, 2016.

[35] Thinking, fast and slow: Kahneman, daniel: Amazon.com.au: Books, https://www.amazon.com.au/THINKING-FAST-SLOW-DANIEL-KAHNEMAN/dp/0374533555.

[36] S. Schöbel, et al., Understanding user preferences of digital privacy nudges – a best-worst scaling approach, 2020.

[37] A. Vedadi, M. Warkentin, "can secure behaviors be contagious? a two-stage investigation of the influence of herd behavior on security decisions ", Journal of the Association for Information Systems (2020) 428–459.

[38] M. E. Poikela, Theoretical Background to Location Privacy, Springer International Publishing, Cham, 2020, pp. 13–32.

[39] C. Olson, K. Kemery, Voice report: Consumer adoption of voice technology and digital assistants, Tech. rep., Technical Report. Microsoft (2019).

[40] S. Gray, Fpf_always_on_wp.pdf, https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf (2016).

[41] E. Zeng, S. Mare, F. Roesner, End user security privacy concerns with smart homes, in: Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security, SOUPS '17, USENIX Association, USA, 2017, p. 65–80.

[42] S. Notra, et al., An experimental study of security and privacy risks with emerging household appliances, in: 2014 IEEE Conference on Communications and Network Security, 2014, pp. 79–84.

[43] H. R. Lipford, et al., Privacy and the Internet of Things, Springer International Publishing, Cham, 2022, pp. 233–264.

[44] S. Yarosh, P. Zave, Locked or not? mental models of iot feature interaction, in: Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI '17, Association for Computing Machinery, New York, NY, USA, 2017, p. 2993–2997.

[45] A. Subahi, G. Theodorakopoulos, Ensuring compliance of iot devices with their privacy policy agreement, 2018, pp. 100–107.

[46] N. Nesa, I. Banerjee, Iot-based sensor data fusion for occupancy sensing using dempster–shafer evidence theory for smart buildings, IEEE Internet of Things Journal 4 (5) (2017) 1563–1570.

[47] E. P. I. C. (EPIC), In the matter of samsung electronics co., ltd., complaint, request for investigation, injunction, and other relief, https://epic.org/privacy/internet/ftc/Samsung/EPIC-FTC-Samsung.pdf (2015).

[48] C. D. Balough, Privacy implications of smart meters, :https://scholarship.kentlaw.iit.edu/cklawreview/vol86/iss1/8 (2010).

[49] Y.-A. Montjoye, C. Hidalgo, M. Verleysen, V. Blondel, Unique in the crowd: The privacy bounds of human mobility, Scientific reports 3.

[50] Q. Huang, K. Rodriguez, N. Whetstone, S. Habel, Rapid internet of things (iot) prototype for accurate people counting towards energy efficient buildings, Journal of Information Technology in Construction 24 (2019) 1–13.

[51] G. Ateniese, et al., Hacking smart machines with smarter ones: How to extract meaningful data from machine learning classifiers, International Journal of Security and Networks 10.

[52] T. Yu, et al., Handling a trillion (unfixable) flaws on a billion devices: Rethinking network security for the internet-of-things, Association for Computing Machinery, New York, NY, USA, 2015.

[53] C. Pathmabandu, J. Grundy, M. B. Chhetri, Z. Baig, An Informed Consent Model for Managing the Privacy Paradox in Smart Buildings, Association for Computing Machinery, New York, NY, USA, 2020.

[54] G. Kumparak, Nest's security system can now be a google assistant | techcrunch, https://tcrn.ch/3Auq9iY (2019).

[55] H. F., Accc's rod sims questions google assurances over fitbit data, https://bit.ly/3QxVmYa (2019).

[56] R. Cronk, Strategic Privacy by Design.

[57] E. Alepis, C. Patsakis, Monkey says, monkey does: Security and privacy on voice assistants, IEEE Access 5 (2017) 17841–17851.

[58] P. G. Hansen, The definition of nudge and libertarian paternalism: Does the hand fit the glove?, European Journal of Risk Regulation 7 (1) (2016) 155–174.

[59] C. Pathmabandu, J. Grundy, M. B. Chhetri, Z. Baig, Icme: An informed consent management engine for conformance in smart building environments, Association for Computing Machinery, NY, USA, 2021.

[60] S. Kvale, S. Brinkmann, Interviews: Learning the craft of qualitative research interviewing, sage, 2009.

[61] V. Braun, V. Clarke, Using thematic analysis in psychology, Qualitative research in psychology 3 (2) (2006) 77–101.

[62] W. C. Adams, et al., Conducting semi-structured interviews, Handbook of practical program evaluation 4 (2015) 492–505.

[63] C. Silva, J. P. Barraca, Dynamic delegation-based privacy preserving in iot architectures, in: 2022 9th International Conference on Future Internet of Things and Cloud (FiCloud), 2022.

[64] G. Ogunniye, N. Kokciyan, A survey on understanding and representing privacy requirements in the internet-of-things, Journal of Artificial Intelligence Research.