An Informed Consent Model for Managing the Privacy Paradox in Smart Buildings

Chehara Pathmabandu
John Grundy
chehara.pathmabandu@monash.edu
john.grundy@monash.edu
Monash University
Australia

Mohan Baruwal Chhetri
Mohan.BaruwalChhetri@data61.csiro.au
CSIRO Data61
Australia

Zubair Baig
zubair.baig@deakin.edu.au
School of Information Technology,
Deakin University
Australia

ABSTRACT

Smart Buildings are defined as the "buildings of the future" and use the latest Internet of Things (IoT) technologies to automate building operations and services. This is to both increase operational efficiency as well as maximize occupant comfort and environmental impact. However, these "smart devices" – typically used with default settings – also enable the capture and sharing of a variety of sensitive and personal data about the occupants. Given the non-intrusive nature of most IoT devices, individuals have little awareness of what data is being collected about them and what happens to it downstream. Even if they are aware, convenience overrides any privacy concerns, and they do not take sufficient steps to control the data collection, thereby exacerbating the *privacy paradox.* At the same time, IoT-based building automation systems are revealing highly sensitive insights about the building occupants by synthesizing data from multiple sources and this can be exploited by the device vendors and unauthorised third parties. To address the tension between privacy and convenience in an increasingly connected world, we propose a user-centric *informed consent model* to foster an accurate user discretion process for privacy choice in IoT-enabled smart buildings. The proposed model aims to (a) inform and increase user awareness about how their data is being collected and used, (b) provide fine-grained visibility into privacy compliance and infringement by IoT devices, and (c) recommend corrective actions through nudges (or soft notifications). We illustrate how our proposed consent model works through a use case scenario of a voice-activated smart office.

CCS CONCEPTS

• **Security and privacy → Privacy protections**; **Human and societal aspects of security and privacy**; • **Social and professional topics → Privacy policies**.

KEYWORDS

IoT, Smart Buildings, Smart Homes, Informed consent, Privacy Preservation, Privacy threats, Voice-assistants, Privacy policies

ACM Reference Format:
Chehara Pathmabandu, John Grundy, Mohan Baruwal Chhetri, and Zubair Baig. 2020. An Informed Consent Model for Managing the Privacy Paradox in Smart Buildings. In *HCSE&CS '20: September, 2020, Melbourne, Australia.* ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/1122445.1122456

1 INTRODUCTION

Smart Buildings (SBs) are buildings that use creative design, smart engineering and information and communication technologies (ICT) to automate and self-regulate their environment and operations [15]. A key feature that differentiates a SB from ordinary buildings is the flexible, automated set of *human-centric* services that it offers. From the moment people step inside, and until the moment they leave, a SB is capable of automatically tracking them at any given time and adjusting its facilities' settings according to their needs, preferences and feedback [32]. The Internet of Things (IoT) is the key enabling technology that transforms normal buildings into "smart" buildings with SBs employing millions of small, diverse, and interactive sensing and actuating devices to automate building operations and services. Market research predicts that by 2025 the total number of connected IoT devices will reach 75.44 billion, representing an increase of 146% from 2020 [28]. Similarly, by 2024, consumers will interact with voice assistants on 8.4 billion devices [19]. There are increasing efforts being made by vendors to design IoT devices so that they can easily be discovered by and commanded through voice-operated and controlled digital assistant platforms. At the same time, the companies behind digital assistant technologies are also seeking new business models to monetize the voice data collected by their platforms [19].

Users of IoT devices claim that they care about the privacy of their data. Nevertheless, research shows that the convenience offered by these devices influences their privacy-related behaviours, and they rarely make active efforts to protect their own information [1]. For instance, when setting up IoT devices, the number of documents one has to review, including the ones related to consent and privacy policies, is quite daunting. Therefore, users tend to use the devices with default settings without looking at the fine print related to the privacy and data collection practices of the device. This discrepancy between the consumers' stated concerns and their actual behaviour is referred to as the *privacy paradox* [29].

According to the GDPR, individuals have the right to control their own data and not have their transactions linked or tracked

HCSE&CS '20, September 2020, Melbourne Australia
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-XXXX-X/18/06…$15.00
https://doi.org/10.1145/1122445.1122456

through IoT devices. In addition, personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed [23]. Given the strict requirements of the GDPR, the collection and provision of legally sufficient consent becomes increasingly difficult. In some cases, smart building IoT solutions cross sectoral and jurisdictional regulatory boundaries and blur the notion of private and public, e.g., data collected in one country but hosted on a cloud in another country. Therefore, there is a real risk that the data collected by IoT devices is shared with third parties, and usually without the knowledge of the users [33]. This data may be retained in transit by a variety of external parties, such as device manufacturers, Government, marketers of products, service providers etc [18] . Unfortunately, most people feel that their privacy is beyond their control and they cannot do anything about it. Therefore, there is a need for a user-centric *informed consent* model, that will (a) increase users' awareness about the privacy invasion and data collection practices of the IoT devices in their home or office environments, (b) provide fine-grained visibility into privacy compliance, and/or infringement by those devices, and (c) recommend corrective actions through nudges (soft notifications).

We are currently exploring ways to protect user data collected from smart devices within SBs – e.g. movement sensors, temperature sensors, light sensors, voice input, user building and room entry, user location, email addresses, calendar schedules, purchases – and the behavioural patterns derived from that data, from unauthorized outsiders and stakeholders. In particular, we are looking at the problems of *lack of informed consent around data capture and usage*, and *user awareness of data capture in smart buildings*. To address these concerns, we seek answers to the following key research questions:

- *RQ1 - What privacy measures have the potential to strengthen the user consent mechanism, and how can their development be promoted?* and
- *RQ2 – How can relevant stakeholders including IoT device manufacturers, Smart Building operators, Internet Service Providers, Government, and Advertising Companies implement better consent mechanisms and user controls to enhance an individuals' ability to provide consent?*

A better understanding of these aspects can inform future smart device design and privacy controls.

The rest of the paper is organised as follows. Section 2 presents a motivating example for our research and provides an overview of related work in the area of privacy, security and privacy paradox in smart IoT devices. Section 3 presents our proposed informed user consent model, and explains how it works through the use of example use-cases. It also briefly summarises the current prototyping efforts within a smart living lab. Section 4 concludes the paper with a discussion of future work.

2 MOTIVATION AND RELATED WORK

2.1 A Voice-activated Smart Office

We consider the example of a voice-activated Smart Office to motivate our research. In smart workplaces, everything is connected and personalised by leveraging advances in IoT, Artificial Intelligence (AI) and Machine Learning (ML), so that employees can be more productive and have better user experiences while working from almost anywhere and at any time. Smart offices connect people to buildings and provide seamless, personalised access to human-centered services. Examples include finding the closest parking lot and working desk, adjusting the lighting and heating settings, reserving a meeting room in advance, and controlling multiple user access by integrating with the calendar system. Fig. 1 illustrates the typical services that an individual working in a smart office would use and interact with on a daily basis. However, to provide such personalised, user-centric services, multiple system components, voice assistants, sensors, smart IoT devices and actuators are required to be interconnected via a communication medium to capture user data consistently. The main objective of capturing user data, including presence, behaviour, and preference data, is to seamlessly enhance user experiences without any human intervention, while operating in the background – as part of the living environment – so that individuals may not even realize that these "smart" devices are there.

Voice and digital assistants are fast replacing touch as the primary user interface [27] and voice is being integrated into everyday appliances used within our homes and offices. Advances in speech recognition technologies have simplified the execution of voice-activated commands, making voice-activated services accessible, progressive, and convenient. The integration of speech recognition brings an array of benefits to consumers of voice-enabled services, both in personal and professional settings. All of the services depicted in Fig. 1 can be voice-activated. Yet, as voice-enabled devices become ever more integrated into our homes, workplaces, and daily routines, the ubiquity of such internet-connected devices is raising many concerns around security, privacy and trust. The voice-activated devices can be generally classified as *manually activated*, *speech activated* or *always on* [14]. Of these, the *always on* devices have the greatest privacy concerns since they operate silently in the background while recording and transmitting data associated with human activities and behaviours at all times. For example, in 2015 privacy advocates lodged a complaint with the FTC (Federal Trade Commission) against Samsung's microphone-enabled Smart TV stating that it was "always switched on" in violation of federal wiretapping laws [9]. 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. Smart appliances including light bulbs, smart switches, door locks and indoor cameras bring along diverse privacy concerns which spill out beyond voice privacy boundaries into other dimensions [5][39][25].

2.2 Related Work

In his seminal work A Theory of Human Motivation, Maslow has identified the "need for privacy" as a core property of self-actualization, which is the highest level of psychological development, i.e., the level at which individuals achieve their full personal potential [20]. A more comprehensive interpretation of privacy encompasses all aspects of an individual's social needs so that privacy can be categorised as *privacy of person*, *privacy of communication*, *privacy of behaviour and action*, and *privacy of personal data* [11]. Clarke defines privacy as "the interest that individuals have in sustaining a 'personal space', free from interference by other people

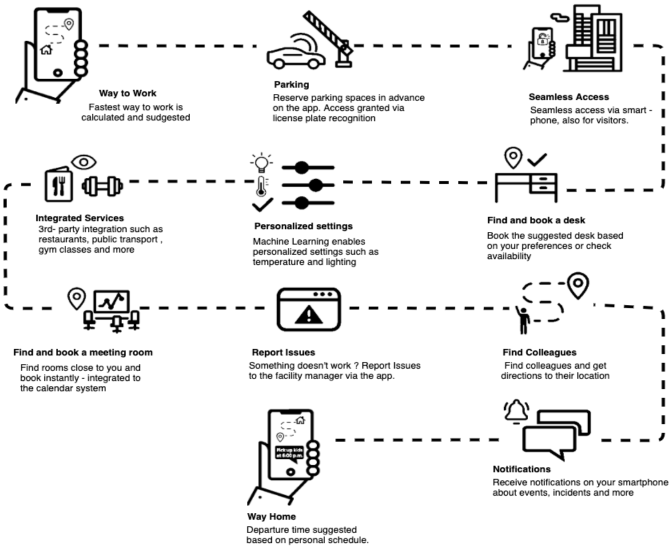
Way to Work
Fastest way to work is calculated and sudgested
Parking
Reserve parking spaces in advance on the app. Access granted via license plate recognition
Seamless Access
Seamless access via smart - phone, also for visitors.
Integrated Services
3rd- party integration such as restaurants, public transport , gym classes and more
Personalized settings
Machine Learning enables personalized settings such as temperature and lighting
Find and book a desk
Book the suggested desk based on your preferences or check availability
Find and book a meeting room
Find rooms close to you and book instantly - integrated to the calendar system
Report Issues
Something doesn't work ? Report Issues to the facility manager via the app.
Find Colleagues
Find colleagues and get directions to their location
Pick up kids at 6:00 p.m.
Notifications
Receive notifications on your smartphone about events, incidents and more
Way Home
Departure time suggested based on personal schedule.

Figure 1: Example of a Voice-activated Smart Office

and organisations" [4]. In the context of smart environments including Smart Buildings it is becoming increasingly critical that every person has the right to control access to his or her personal information, and is aware of who is collecting their data, for how long, and for what purpose [3].

Therefore, getting user consent is crucial for improving user awareness about how their data is being collected and used and to provide visibility into privacy compliance. While *Consent* is frequently used as a justification for businesses to use and disclose personal information, valid consent requires more than making a user click 'I agree'. According to the Australian Privacy Principle Guidelines [26], meaningful consent has the following five aspects – *capacity*, *voluntary*, *current and specific*, *informed* and *expressed* or *implied* [26]. An individual, or a guardian in case of a minor, must be capable of giving consent for it to be valid (*Capacity*). Consent must be a genuine choice that was freely given (*Voluntary*). For instance, forcing workers to wear IoT wristbands to monitor their performance [38], using smart badges to monitor the nature of the conversations of call centre staff [13], and placing chemical sensors on doctors to ensure they wash their hands enough [30] 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*). Therefore, an informed consent model for data collection and sharing in Smart Buildings should address these five aspects.

However, the discrepancies between user attitude and their actual behaviour related to privacy concerns obscure their decision-making and creates conflict between the interests of consumers and providers [37]. The trade-off between the disclosure of personal information and service-related benefits leads to the *privacy paradox in IoT*. A possible reason why consumers are willing to trade away their privacy is that they are unaware of the amount of privacy that is being lost [3]. Even if consumers were made aware of the loss, they would still engage in privacy-sacrificing behaviours. Some researchers and organizations have made a series of attempts to improve this situation by managing access control and permissions granted by the user to IoT devices. Notable examples include AppOps [8] and Norton AppAdvisor [24]. Both applications directly fetch OS-level permissions for their analysis and allow users to grant or deny permissions for installed apps selectively. 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 and other privacy risks associated with the app. However, *neither of them compares the IoT data payloads with the agreed privacy policy statements to detect any violations*. Furthermore, several smart home automation open-source tools are available for users to exercise control locally over the smart devices and their data flow in their personal environments without any interventions from a third party. Home Assistant [36] and OpenHAB [35] are some of the tools which consider privacy as their fundamental priority.

Recently, researchers have demonstrated how a low-cost Raspberry Pi-based device can warn users when a voice assistant snoops on people without their consent [21]. Though they address the same privacy concern, the approach that we present comes from the design which can be applied to any IoT device and any scenario with a conclusive legal explanation. They detect if a device is unexpectedly recording and sending audio to the Internet without waking up the device, whereas, we initiate our design with an edge case (only after waking up the device) and can be applied for any personal identifiable information (PII), including audio streams. They check the sudden increase of traffic rates in audio-related events at any time whereas, we check the payloads when a user triggers an event. Also, they do not consider checking the policies related to the audio recording of the device while we scan all the events with the defined policies of the device.

3 CONCEPTUAL ARCHITECTURE

In this section, we present a conceptual architecture for our proposed *informed consent model* that allows users to self-track what they do within their respective smart spaces. We first outline the key requirements for an informed consent model for IoT device users. Following this, we present a conceptual architecture for informed consent and discuss the key phases leading to informed consent. Finally, we use some example use cases to illustrate how the consent model can be realized.

3.1 Key Requirements

To identify the key requirements for an informed consent model for IoT device users in smart buildings or homes, we first performed a systematic review of relevant literature. We analysed 72 relevant primary studies to get a better understanding of the current privacy gaps in SBs that use smart voice-assisted devices. The key finding from the study was that there is 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.

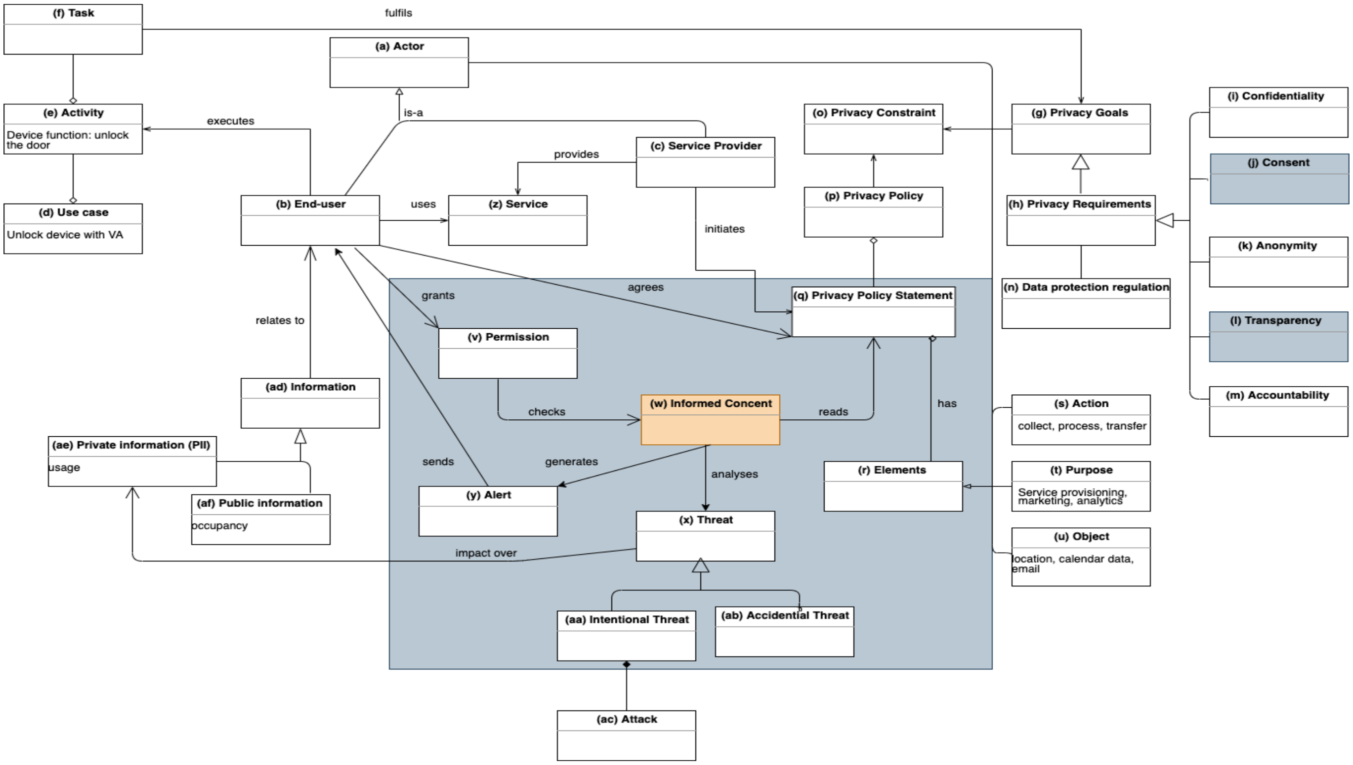

Figure 2: Conceptual model for informed consent in Smart Building devices

Following this literature review, we identified the following key requirements for an informed consent model:

- *Track data collection approaches when activating permissions to consume "smart services" – i.e. determine for each smart device what data it collects, how, when, about who and what privacy implications this data may have;*
- *Label data as sensitive and non-sensitive – e.g. temperature in room changing may unintentionally reveal person presence;*
- *Record existing privacy settings and data sharing practices of each user – to provide them ongoing awareness;*
- *Structural representation for privacy policies – i.e. how do we define the user, team, organisational privacy policies in the presence of the smart devices as per Figure 2;*
- *Ensure the maintenance of a meaningful informed consent with all five elements – when new/changed/integrated device data capture is about to occur, proactively highlight to the user to ensure their consent, especially in the context of multiple device data capture;*
- *Revise dynamic/ongoing consent – as user moves, new devices are encountered, data capture begins/changes, new user enters room, etc.; and*
- *Address relevant privacy by design (PbD) principles that the consent model addresses – see discussion below.*

In designing the consent model, we have addressed the following five foundational principles of *privacy by design* [7]. How each principle is addressed via the proposed design is explained below.

- PR1 – *proactive, not reactive; preventative, not remedial* – Privacy considerations need to help drive the design, and not the reverse where the design drives detection and highlighting of privacy violations. Our proposed consent model creates an environment for the end-user to provide proactive actions to control the disclosure of their data, limiting potential privacy infringements. Thereby, any future complaints on unauthorized aggregation or use of consumer data; monetary penalties for deceptive practices; data privacy programs that are subject to biennial third-party audit requirement; deletion of consumer information that had collected unfairly, in violation of notice and choice principles will be diminished gradually.
- PR2 – *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 is about understanding the context tacit between participants. The consent model we propose cross-checks the user-granted access permissions 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. For instance, grant access to calendar data where it is not defined in the permission list of the device upon publishing the app.
- PR3 – *privacy embedded into design* – this states that privacy must be inseparable to the design so that the system or process would not function without the 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. Therefore, privacy is embedded in the

consent model, making it integral while preventing the consumer from submitting personal information without consent.

- PR4 – *visibility and transparency* – Pushing consent-seeking "nudges" to the end-user with a full justification about the collection or use of PII increase visibility. This information is necessary to decide on granting permission to service, to moderate their behaviour or to use the model recommended corrective actions to reduce privacy risks.
- R5 – *respect for user privacy by keeping it user-centric* – Every user is different in terms of their privacy expectations. *PR5* says that we need to allow each user the ability to define their own privacy expectations for work context, location, set of devices, time of day, activity, and so on.

3.2 Conceptual Architecture

To fulfil the above requirements we propose a conceptual architecture for an informed consent model, as shown in Fig. 2. There are two key actors involved in our consent model – the *end-user* (a) and the *service provider* (c). Both actors may depend on each other for accomplishing their objectives. The end-user executes multiple *tasks* (f) associated with the device-specific *activities* (e) related to a particular *use case* (d). For example, *an employee unlocking the smart lock on the front door of the smart office via his voice assistant. After finding a free desk space, the employee may adjust the smart lights to meet his preferences with a single command* (refer to the scenario presented in Section 2.1).

A set of *privacy goals* (g) have to be fulfilled when executing the service provider-defined tasks. 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* (n). In our context, it is essential to understand the privacy goals of the stakeholders. In particular, unlinkability, intervenability and transparency have been considered in our model [31]. Referring to the example in Section 2.1, *employees have the right to know whether their personal preferences, working hours, and entry and exit times are monitored or tracked from their daily engagements with the smart devices.* Furthermore, the privacy requirements can be further refined as *Confidentiality* (i), *Consent* (j), *Anonymity* (k), *Transparency* (l) and *Accountability* (m). Though each factor is equally important, in our informed consent model, we will be mainly focusing on enhancing user consent and transparency throughout the data life-cycle.

End-users (b) consume the *service* (z) provided by the dedicated *service providers* (c) of the smart devices. Moreover, all the applicable *privacy policy statements* (q) of these devices are initiated by their service providers. They generate policy documents for every device or device group aligning with applicable data protection laws and regulations to date. These privacy policy statements are mostly found during 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 reservation based on the participant 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 (e.g. turning Nest Secure's keypad hub into a Google Home Mini) [17]. An IoT vendor might be acquired by a different organisation that has an entirely different set of privacy policies or could collect and use personally identifiable information (PII) for new purposes that current users may not have contemplated (e.g. Google's Policy with Fitbit Data) [10]. Therefore, end-users need to have the full right to agree or disagree on policies related to the use and setup of their devices.

There are several research works that have discovered that lengthy full-text policies cause disadvantages in 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 [22], a labelled grid layout [16], symbolic visualization [12], and various other tools [34] and policy editors [6] for the generation of privacy policy statements. These solutions aim to improve the comprehensibility of the text in privacy policies and address the incompleteness in the information presented to the end-users with respect to privacy practices. By leveraging these solutions, we can partition policy statements into four *elements* (r) as presented in Fig. 2. Referring to the example in Section 2.1, *Employees who have consented to share their sensitive information should (a) have visibility into who monitors, collects, and uses their data, and (b) the right to withdraw their consent at any time.*

The *threat* (x) captures events that can potentially threaten PII by misusing a vulnerability concerning such information. Based on the severity of the impact, threats can be characterized as high, medium or low. A threat can be either natural, accidental, or intentional. Therefore, threats are represented as *accidental* (ab) and *intentional* (aa) threats in our model. Referring to the example in Section 2.1, *analysing an employee's data overtime may reveal insights of working patterns, personal habits, power consumption, medical conditions, search history, social connections and presence which may cause a potential gateway for intentional threats.*

When the *end-user* triggers an action, and *permission* (v) needs to be granted to a *service* (z), the *informed consent engine* (w) will check the permissions granted by the user against the privacy policy statements of a given device. If the consent engine detects any policy infringements, they are recorded to maintain the event history and for future purposes. Finally, the consent engine notifies the end-user through an *alert* (y) (or *soft nudge*) to make them aware of the policy infringement.

3.3 Applying the Informed Consent Model

Applying our model involves the following five key phases:

3.3.1 Phase 1: Apply textual patterns to privacy policies.

Privacy policies of the used devices are read and converted into an appropriate human and machine-readable format (e.g. JSON, XML). Next, privacy policy statements of selected IoT devices are categorized into four elements(<User><Action><Data><Purpose> compliance with <Privacy policy>) [22]. For instance, the service provider collects end-user data (usage frequency/level of settings) for service provisioning/analytics . This interpretation enhances the readability and transparency between the service provider and the end-user.

This mechanism assists in better understanding the data collection practices and transferring the risk.

3.3.2 *Phase 2: List privacy permissions.*

The consent management engine reads the current permissions granted by the user of each device. All of the permissions defined by the device manufacturers need to be checked to have more visibility into the personal data that the vendor can collect about the device user. Following this, possible dangerous permissions that have the risk of revealing sensitive information about the users, which can be used for profiling, tracking, advertising and identification [2] need to be identified, labelled and listed.

3.3.3 *Phase 3: Identify privacy infringements.*

In this phase, payload data for each user executed action is captured, and potentially preprocessed into a lightweight data-interchange format that is both human and machine-readable. This data is then compared against the structured policy statements obtained from Phase 1 to identify and record policy breaches before being passed on to Phase 4.

3.3.4 *Phase 4: Track and log events.*

All of the actions (events, actions, time, current status) are tracked and logged. These details will be analysed further with the output of Phase 3 to send statistical nudges to the user informing what has been inappropriately collected or shared by the devices infringing the privacy policies. This approach will gradually enhance user awareness and visibility.

3.3.5 *Phase 5: Recommend preventive actions and nudge user.*

Finally, corrective actions are recommended to the user to control and mitigate emergent privacy issues that have occurred and/or may transpire in future. A nudge consists of three elements: (1) redirecting instructions to the privacy settings wireframe, (2) a summary of the unauthorised actions, (3) ignore and allow data to be shared options. 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 so 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 will foster an accurate user discretion process for privacy choice in fading existing privacy paradox. Moreover, the consent engine flags possible privacy vulnerability alerts with the occurrence of unintended movements, activation of devices, enablement of permission within the SB premises.

3.4 Example Use Cases

Below we illustrate our proposed approach using three scenarios to describe how our consent model is used to help end-users improve their privacy-related behaviour in a smart building by nudging them to take corrective actions and to update their device privacy settings. Fig. 3 shows an example flow of the main interactions between the different components in the consent model and the high-level flow of operations for Scenario 1. We consider three different ways in which the IoT device can be controlled and illustrate how our consent model works with them: **(A)** – the user uses a dedicated app provided by the IoT device vendor to trigger actions on the IoT device; **(B)** – a voice assistant triggers the action on behalf of the user; **(C)** – the user uses an automation tool that supports devices from different vendors (e.g. Home Assistant [36] or OpenHAB [35]) to control the IoT device.

Scenario 1: End-user Mohan uses a smart lighting system that can be controlled through an app, via a voice assistant (VA) and via an automation panel in a smart living lab. His location data is obtained using his mobile phone's geolocation technology and integrated with the usage of the smart lighting system. Based on his voice commands, the lights can be switched on and off, or dimmed (Fig. 3, Data flow B - 1). At the same time, his location information can be used to learn about his availability. The informed consent engine will analyze the granted permissions, applicable policies, threat level of the disclosed PII and notify Mohan with a detailed summary of how his data is being captured and used (Fig. 3, Data flow B - 2). An example notification may look like – *your geolocation details have been shared with six other apps and two stakeholders 128 times for the last 14 days.* Based on this notification, Mohan can decide whether to take preventative actions to stop the flow of his geolocation data, for instance by disconnecting the device or putting the device behind a 'firewall' as the data might not be encrypted or anonymised. Fig. 3 shows how the consent engine will track the user initiated actions and nudge the user appropriately under the three different settings.

Scenario 2: John works in a Smart Office and the Smart Door Lock is connected to his phone and can access his calendar. John can control the lock using the associated app, using a voice assistant and also through the nudge application/automation panel. The nudge application/automation panel will sense and track John's smart door lock, which is connected to his phone, access his calendar data through the mobile phone's read calendar technology and also, it can be controlled via a VA device (e.g. Google Home). The usage patterns of door locks are used to target localised advertising about its modern functionalities (e.g. multiple access solutions based on calendar schedules/meetings/availability). Based on controls set up through privacy settings of the app by John, this activity will either inform or nudge John for possible actions that include closing the port through which the calendar data flows.

Scenario 3: In this scenario, the nudge application/automation panel makes Zubair aware of unintended data flowing through one or more channels to a third-party server overseas (e.g. Smart TV usage data via his Wi-Fi network). Based on the notification, Zubair might choose to formally consent to this data sharing or report the unauthorised behaviour to an appropriate regulatory entity.

3.5 Progress

We are currently prototyping our model with non-commercial smart devices and peripherals. We have "mocked-up" several smart device interfaces, i.e., write "device interfaces" that are not real devices but mimic their behaviours. (e.g. Smart Bulb, Smart Lock). We will connect these devices with an open-source IoT control panel such as Home Assistant [36] or OpenHAB [35] and integrate the control panel with a private cloud-based MQTT instance. MQTT broker creates a communication medium for the devices and provides a lightweight method for carrying out messaging using a publish-subscribe model. We will capture messages, i.e., the payload data,

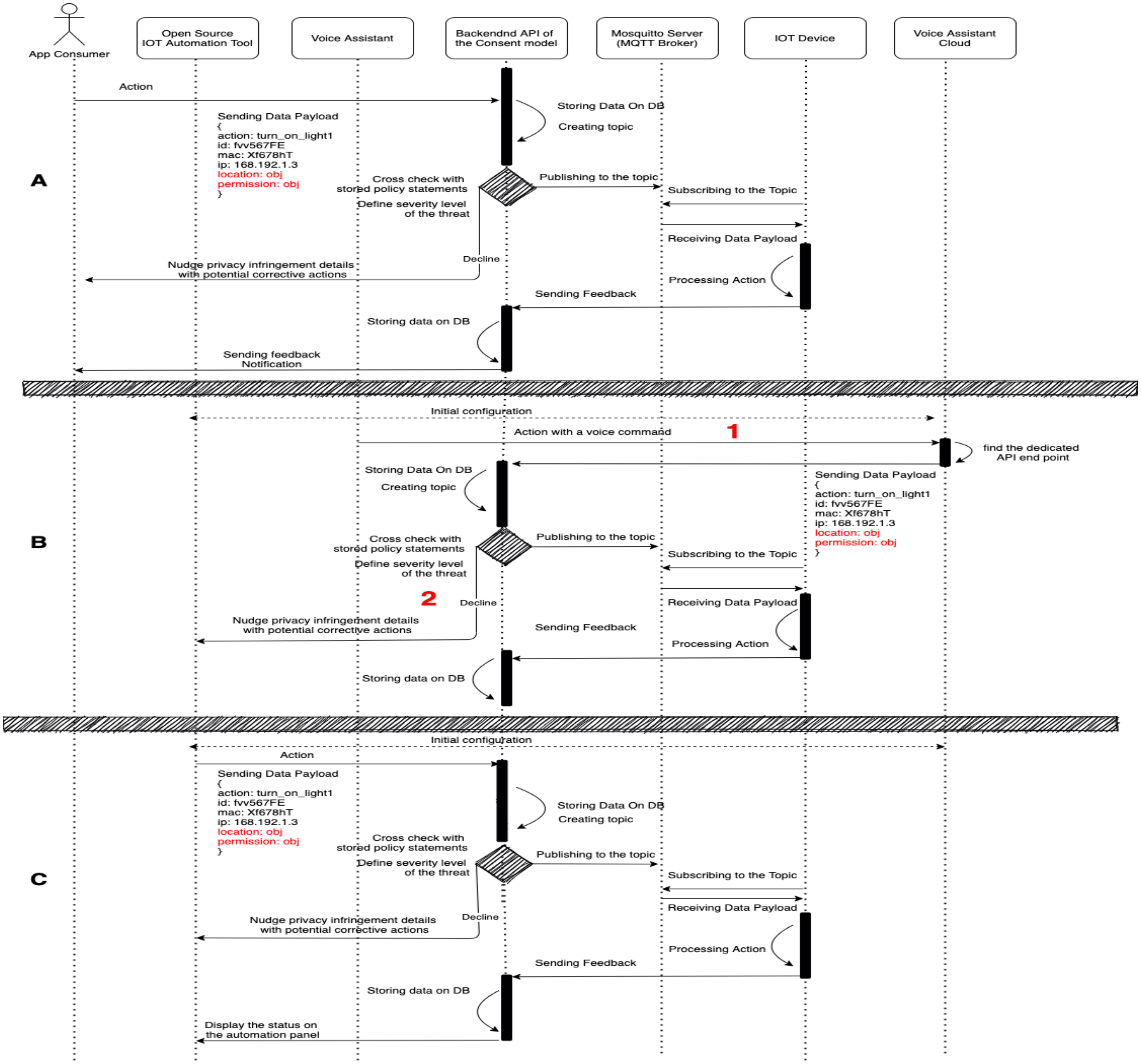

Figure 3: Sequence Diagram showing Scenario 1 key data flows: A – an IoT device app user controlled interaction; B – a voice controlled device linked to an automation tool; and C – a hub or an IoT automation tool controlled device

to monitor whether they include any sensitive data (user location, availability, calendar data or any other PII), which may violate the initial user consent given upon access permission. This is compared with the structured privacy policy statements while measuring the severity level of the threat. Finally, a detailed privacy policy violation nudge is released to the user with a recommendation of potential corrective actions. An agile prototyping approach is being used to build and test the current prototype version of the informed consent model to receive continuous feedback on the level of awareness and usability. We test whether the model triggers a nudge when we feed or request additional PII data from the end-user, which is not defined in the policy statements. Furthermore, we use our example scenarios above to evaluate this feasibility study. We are currently working on applying textual-patterns to the policy statements, as explained in3.3.1, and as the next phase, we will focus on identifying privacy infringements and creating the nudge content.

4 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 individuals without their informed consent. Our recent literature review on privacy in IoT-driven Smart Buildings has identified that there are a number of research gaps. These include lack of enforcement of privacy policies, lack of providing mechanisms for informed user consent, poor addressing of unintended data collection, use, retention and disclosure, and lack of definition of the exact limits of smart device data capture and usage. In this paper, we presented a novel informed consent model that seeks to address some of these research challenges. We first enumerated some of the key requirements for an informed consent model and then proposed a conceptual framework and architecture that addresses some of these requirements. We used example use cases to illustrate how the proposed model might (a) enhance user awareness and transparency, (b) help detect privacy compliance and infringement by IoT devices, and (c) improve users' privacy-protecting behaviours through soft nudges. We are currently developing a prototype implementation of the proposed conceptual architecture as a feasibility study to envisage a smart building set up and to facade the mock-ups to real devices later. Our future work will focus on developing appropriate nudging strategies to be used within the consent model. We will also integrate commercial IoT devices with our user consent model.

ACKNOWLEDGMENTS

This work is supported by a CSIRO/Data61 PhD scholarship. Grundy is supported by ARC Laureate Fellowship FL190100035.

REFERENCES

[1] Noura Aleisa, Karen Renaud, and Ivano Bongiovanni. 2020. The privacy paradox applies to IoT devices too: A Saudi Arabian study. *Computers Security* 96 (2020), 101897. http://www.sciencedirect.com/science/article/pii/S0167404820301711

[2] E. Alepis and C. Patsakis. 2017. Monkey Says, Monkey Does: Security and Privacy on Voice Assistants. *IEEE Access* 5 (2017), 17841–17851.

[3] Krystan Berg, Ton Spil, and Robin Effing. 2019. *The Privacy Paradox of Utilizing the Internet of Things and Wi-Fi Tracking in Smart Cities.* 364–381.

[4] Roger Clarke. 2006. What's' Privacy'. In *Australian law reform commission workshop*, Vol. 28.

[5] Federal Trade Commission)(FTC). 2019. In the Matter of TAPPLOCK, INC, Complaint, Request for Investigation, Injunction, and Other Relief. https://www.ftc.gov/system/files/documents/cases/192_3011_tapplock_complaint.pdf.

[6] IBM Corp. 2002. IBM P3P Policy Editor. https://www.w3.org/P3P/imp/IBM/. (Accessed on 08/04/2020).

[7] R.J. Cronk. 2018. *Strategic Privacy by Design.* International Association of Privacy Professionals. https://books.google.com.au/books?id=TPH5uwEACAAJ

[8] Google Developers. 2014. AppOpsManager | Android Developers. https://developer.android.com/reference/android/app/AppOpsManager. (Accessed on 08/07/2020).

[9] Electronic Privacy Information Center (EPIC). 2015. 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.

[10] Hunter F. 2019. ACCC's Rod Sims questions Google assurances over Fitbit data. https://www.smh.com.au/politics/federal/it-is-a-stretch-accc-s-sims-questions-google-assurances-over-fitbit-data-20191119-p53by8.html.

[11] Rachel L. Finn, David Wright, and Michael Friedewald. 2013. Seven Types of Privacy. In *European Data Protection.*

[12] Kambiz Ghazinour and Tahani Albalawi. 2016. A Usability Study on the Privacy Policy Visualization Model. *2016 IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, 14th Intl Conf on Pervasive Intelligence and Computing, 2nd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)* (2016), 578–585.

[13] V. Giang. 2013. Companies Are Putting Sensors On Employees To Track Their Every Move | Business Insider. https://www.businessinsider.com.au/tracking-employees-with-productivity-sensors-2013-3?r=US&IR=T.

[14] Stacey Gray. 2016. FPF_Always_On_WP.pdf. https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf. (Accessed on 07/31/2020).

[15] Aurecon Group. 2020. What is a smart building? | Aurecon | Buildings of the future. https://www.aurecongroup.com/expertise/digital-engineering-and-advisory/smart-buildings.. (Accessed on 06/12/2020).

[16] Patrick Gage Kelley, Lucian Cesca, Joanna Bresee, and Lorrie Faith Cranor. 2010. Standardizing Privacy Notices: An Online Study of the Nutrition Label Approach. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (Atlanta, Georgia, USA) *(CHI '10)*. Association for Computing Machinery, New York, NY, USA, 1573–1582.

[17] G. Kumparak. 2019. Nest's security system can now be a Google Assistant | TechCrunch. https://techcrunch.com/2019/02/04/nests-security-system-can-now-be-a-google-assistant/?guccounter=1.

[18] Milan Markovic, Waqar Asif, David Corsar, Naomi Jacobs, Peter Edwards, Muttukrishnan Rajarajan, and Caitlin Cottrill. 2018. Towards automated privacy risk assessments in IoT systems. 15–18.

[19] Chuck Martin. 2020. Voice Assistant Usage Seen Growing To 8.4 Billion Devices 04/28/2020. https://www.mediapost.com/publications/article/350643/voice-assistant-usage-seen-growing-to-84-billion.html. (Accessed on 07/29/2020).

[20] A. H. Maslow. 1943. A Theory of Human Motivation. *Psychological Review* 50, 4 (1943), 370–396.

[21] Richard Mitev, Anna Pazii, Markus Miettinen, and William Enck and. 2002. LeakyPick: IoT Audio Spy Detector. https://arxiv.org/pdf/2007.00500.pdf. (Accessed on 08/08/2020).

[22] Nazila Mohammadi, Jens Leicht, Ludger Goeke, and Maritta Heisel. 2020. Assisted Generation of Privacy Policies using Textual Patterns. 347–358.

[23] Privacy Europe International Network. 2018. General Data Protection Regulation(GDPR). https://gdpr-info.eu/.

[24] NortonLife. 2020. App Advisor feature in Norton Mobile Security. https://support.norton.com/sp/en/au/home/current/solutions/v97499944. (Accessed on 08/07/2020).

[25] S. Notra, M. Siddiqi, H. Habibi Gharakheili, V. Sivaraman, and R. Boreli. 2014. An experimental study of security and privacy risks with emerging household appliances. In *2014 IEEE Conference on Communications and Network Security.* 79–84.

[26] OAIS. 2019. Australian Privacy Principles guidelines, Chapter B: Key concepts. https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/#consent.

[27] Christie Olson and Kelli Kemery. 2019. *Voice report: Consumer adoption of voice technology and digital assistants.* Technical Report. Technical Report. Microsoft.

[28] Robert Oshana and Mark Kraeling. 2019. *Software engineering for embedded systems : methods, practical techniques, and applications* (second edition. ed.).

[29] Karen Renaud, Ivano Bongiovanni, and Noura Aleisa. [n.d.]. The privacy paradox: we claim we care about our data, so why don't our actions match? https://theconversation.com/the-privacy-paradox-we-claim-we-care-about-our-data-so-why-dont-our-actions-match-143354. (Accessed on 07/31/2020).

[30] M. Rhodes. 2014. A Gadget Designed to Finally Make Doctors Wash Their Hands Enough | WIRED. https://www.wired.com/2014/08/a-gadget-designed-to-finally-make-doctors-wash-their-hands-enough/.

[31] Pfitzmann A. Rost, M. 2009. Data protection goals - revisited | SpringerLink. https://link.springer.com/article/10.1007/s11623-009-0072-9.

[32] Nico Saputro, Ali Yurekli, Kemal Akkaya, and Selcuk Uluagac. 2016. *Privacy Preservation for IoT Used in Smart Buildings.* 129–160.

[33] Mohamed Seliem, Khalid Elgazzar, and Kasem Khalil. 2018. Towards Privacy Preserving IoT Environments: A Survey. *Wireless Communications and Mobile Computing* 2018 (11 2018), 15.

[34] Alberto Silva, João Caramujo, Shaghayegh Monfared, Pavel Calado, and Travis Breaux. 2016. Improving the Specification and Analysis of Privacy Policies - The RSLingo4Privacy Approach. 336–347.

[35] Eclipse SmartHome. 2010. openHAB. https://www.openhab.org/. (Accessed on 08/07/2020).

[36] Home Assistant Core Team and Community. 2013. Home Assistant. https://www.home-assistant.io/. (Accessed on 08/07/2020).

[37] M. Williams, J. R. C. Nurse, and S. Creese. 2016. The Perfect Storm: The Privacy Paradox and the Internet-of-Things. In *2016 11th International Conference on Availability, Reliability and Security (ARES).* 644–652.

[38] C. Yeginsu. 2018. If Workers Slack Off, the Wristband Will Know. (And Amazon Has a Patent for It.) - The New York Times. https://www.nytimes.com/2018/02/01/technology/amazon-wristband-tracking-privacy.html.

[39] Eric Zeng, Shrirang Mare, and Franziska Roesner. 2017. End User Security Privacy Concerns with Smart Homes. In *Proceedings of the Thirteenth USENIX Conference on Usable Privacy and Security* (Santa Clara, CA, USA) *(SOUPS '17)*. USENIX Association, USA, 65–80.