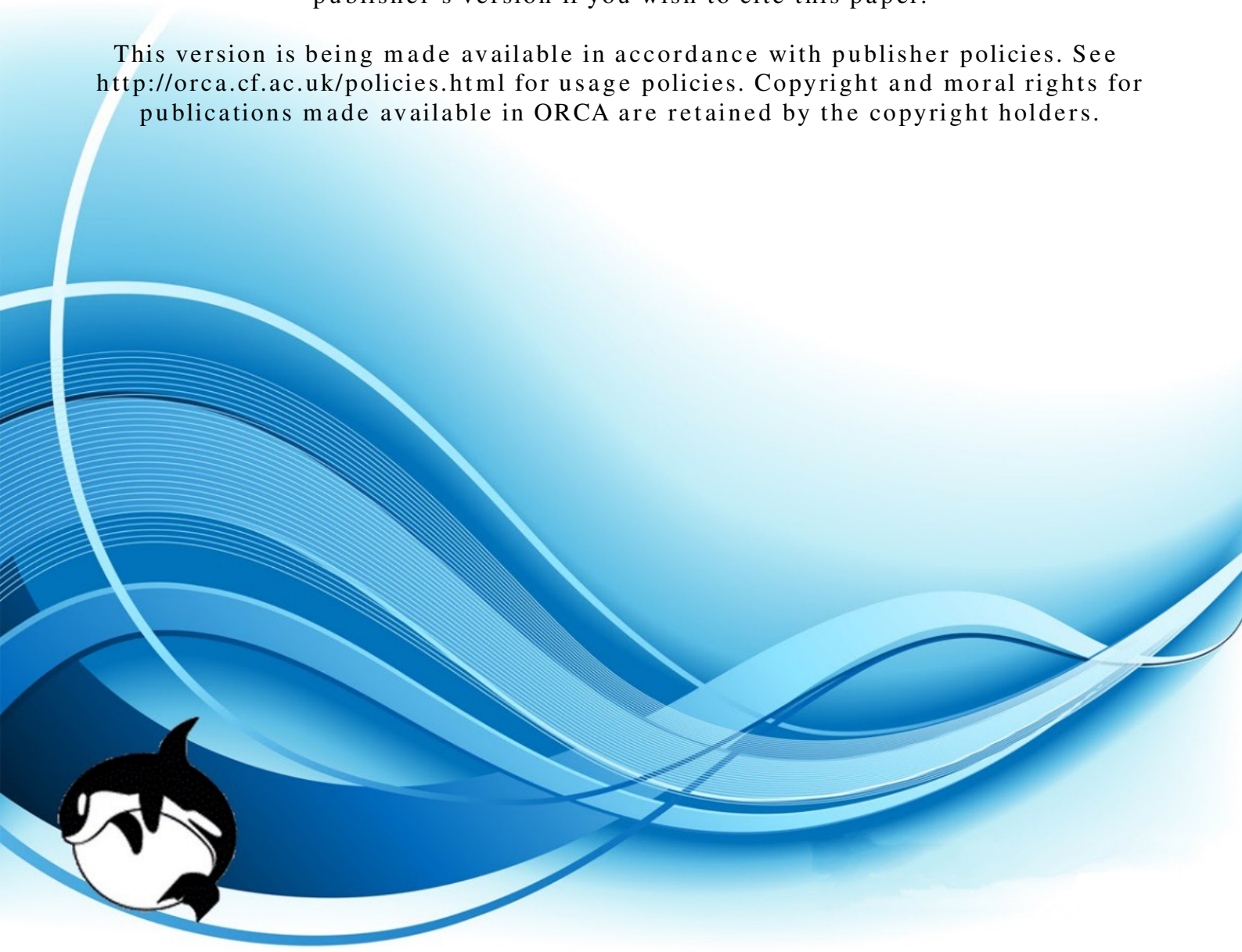

Interactive Privacy Management: Towards Enhancing Privacy Awareness and Control in Internet of Things

BAYAN AL MUHANDER, Cardiff University, UK
JASON WIESE, University of Utah, US
OMER RANA, Cardiff University, UK
CHARITH PERERA, Cardiff University, UK

The balance between protecting user privacy while providing cost-effective devices that are functional and usable is a key challenge in the burgeoning Internet of Things (IoT). While in traditional desktop and mobile contexts, the primary user interface is a screen, in IoT devices, screens are rare or very small, invalidating many existing approaches to protecting user privacy. Privacy visualisations are a common approach for assisting users in understanding the privacy implications of web and mobile services. To gain a thorough understanding of IoT privacy, we examine existing web, mobile, and IoT visualisation approaches. Following that, we define five major privacy factors in the IoT context: (i) type, (ii) usage, (iii) storage, (iv) retention period, and (v) access. We then describe notification methods used in various contexts as reported in the literature. We aim to highlight key approaches that developers and researchers can use for creating effective IoT privacy notices that improve user privacy management (awareness and control). Using a toolkit, a use case scenario, and two examples from the literature, we demonstrate how privacy visualisation approaches can be supported in practice.

CCS Concepts: • **Human-centered computing** → **Interaction paradigms**; **Ubiquitous and mobile computing**; • **Security and privacy** → *Human and societal aspects of security and privacy*.

Additional Key Words and Phrases: Internet of Things, sensors, privacy awareness, notification methods, privacy management, privacy control, choice, interaction, visualisation.

ACM Reference Format:
Bayan Al Muhander, Jason Wiese, Omer Rana, and Charith Perera. 2023. Interactive Privacy Management: Towards Enhancing Privacy Awareness and Control in Internet of Things. *J. ACM* 9, 9, Article 9999 (September 2023), 34 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

The built environment is currently undergoing a rapid transformation as shared spaces [18, 46], e.g., transport, commercial and residential buildings, are being infused with sensors [5, 57, 102]. Fueled by the proliferation of the Internet of Things (IoT) sensors, it is estimated that in 2025 "each connected person will have at least one data interaction every 18 seconds" [131]. Each of these interactions has the potential to be recorded, analyzed and shared. As the vast majority of these interactions are invisible, they pose several privacy risks to individuals, e.g. when a person walks into a "smart" shared space, they have no way of knowing what technology is present, what

Authors' addresses: Bayan Al Muhander, Cardiff University, UK, almuhanderb@cardiff.ac.uk; Jason Wiese, University of Utah, US, wiese@cs.utah.edu; Omer Rana, Cardiff University, UK, RanaOF@cardiff.ac.uk; Charith Perera, Cardiff University, UK, pererac@cardiff.ac.uk.

0360-0300/2023/9-ART9999 $15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

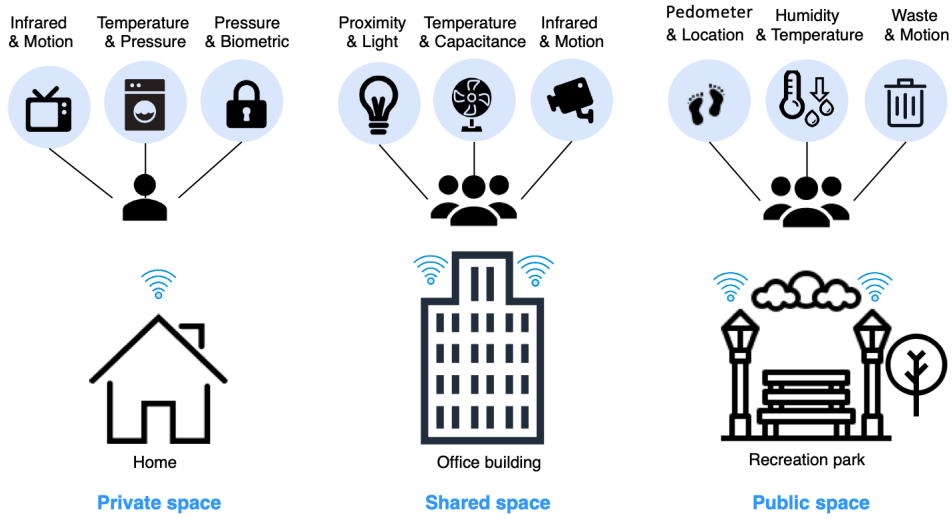

Fig. 1. IoT sensors employed in various spaces, which collect individuals' data without their knowledge.

data is collected, or what happens to that data. Moreover, controlling such IoT sensors following individuals' privacy preferences is another challenge. Figure 1 shows how IoT sensors can collect data about individuals in various spaces without their knowledge.

Several studies have discussed **user-centred privacy management**, which includes both privacy awareness and privacy control (we use the term privacy management to refer to both privacy awareness and control). Privacy awareness involves notifying individuals about the collection and use of their data, whereas privacy control allows individuals to configure certain aspects of their privacy preferences. Studies have also shown that effective privacy notices provide individuals with privacy awareness, allowing them to make informed privacy decisions and have better control over their data [25, 77, 126]. However, managing IoT privacy has a greater degree of potential options than managing web or mobile application privacy. First, IoT devices collect critical amounts of personal private data [168]. Second, IoT devices interact with multiple systems and with numerous users who have varying privacy preferences [110]. Third, IoT devices perform/provide sensitive tasks or services [165]. Moreover, most IoT privacy notices are presented in two formats. A privacy notice sign, such as a CCTV camera in operation may go unnoticed and reveal no information about what happens to the collected data [28]. Alternatively, a privacy policy document with a long list of policies in which users provide their consent but fail to read [1, 64, 82]. Furthermore, users frequently report having difficulty modifying their privacy preferences, due to a lack of clarity on how privacy configuration options can be updated or visualised.

As a result of the aforementioned difficulties, several studies have been conducted to investigate the importance of individuals' privacy awareness and control. The challenges that individuals face when making privacy decisions and the difficulties that developers face when attempting to comply with privacy policies are discussed in [6, 100, 127, 144, 167]. Individual behaviour and how privacy awareness can be raised in the context of IoT have been studied and analysed by [8, 80, 93, 113, 156, 160]. Studies that support privacy awareness by analysing user preferences and reactions to notifications are presented in [1, 97, 134, 135, 159].

It is important to note that previous approaches provide limited ways of improving user privacy management, focused on web and mobile platforms, or are targeted at specific, usually technical,

users. Further, the majority of prior studies did not concentrate on mapping the many elements involved in conveying and providing users with access to privacy options. Information disclosure is more complicated in the IoT domain because of the wide distribution and passive capability of collecting information about people [103, 111]. We present this survey as a comprehensive literature review of privacy management options that could be used in the context of IoT.

We examined the privacy management options available on the web and mobile platforms and identify common themes with IoT systems. This enabled us to identify five key factors that must be considered when presenting IoT privacy management options to the user: (1) data type, (2) data usage, (3) data storage, (4) data retention, and (5) data access. These factors typically have different framing and presentation, which could further influence user privacy management. This paper discusses each of these factors, as well as their various modalities. Our goal is to identify critical factors that the IoT domain should support, particularly when creating a privacy-managed environment. Using a literature review, we develop a taxonomy of common factors and present several examples from the literature. We compare research findings and efforts, identify gaps, and highlight challenges. This paper contributes to the existing literature in the following way:

- Review available web, mobile and IoT techniques. These include protocols and models reported in the literature on privacy awareness and control with the intention of proposing a toolkit for IoT designers and developers.
- Distill privacy management factors and define them in the context of IoT.
- Create and apply a taxonomy to classify existing literature on notification visualisation.
- Propose a privacy management toolkit and demonstrate its use with a use case scenario and two examples from the literature.

*P*aper structure: The paper is divided into eight sections and is structured as follows: the followed search methodology is described in Section 1.1. Section 2 provides background information on techniques and protocols used for web and mobile privacy. Section 3 presents information on existing models used for IoT privacy. Section 4 is divided into five main subsections, each of which discusses one of the main factors pertaining to individuals' awareness and control. The five subsections are data type, usage, storage, retention, and access. In Section 5, we present several works of literature investigating notification methods in different contexts and propose a privacy management design toolkit with a use-case scenario and two examples from the literature on its application. In Section 6 we include a discussion about IoT awareness and control and present the gaps in this area. Section 7 includes a discussion of research challenges and opportunities, with Section 8 concluding the survey.

1.1 Methodology

This survey results from a thorough review of the literature in the area of privacy awareness and control. In this paper, we draw on the results and findings in this area to provide an organised summary of the available privacy visualisations that are (or can be) incorporated into the IoT domain. To build this survey, we performed several steps as follows:

First, we used a search strategy to find relevant articles in the databases of the Association for Computing Machinery (ACM), IEEE Xplore digital library, ScienceDirect, and SpringerLink. We used the search queries tabulated in Table 1. To avoid publisher bias, we further expanded our search with Google Scholar to find valuable grey literature. Our initial Google Scholar search using the keywords in Table 1 yielded many thousands of articles (222,400 results). To reduce scope, we repeated the search concentrating on specific keywords, as shown in Table 1. The preceding returned 6158 results. We limited our search to research articles on ScienceDirect and proceedings and research articles on ACM. In the IEEE and SpringerLink databases, we narrowed our search

to only include conferences. We excluded review articles from the Google Scholar database. We filtered the publication date to (2016-2022) and the language to English in all databases. The results of these queries were combined and sanitized for duplicates.

After that, we manually screened the articles by reading only the titles as a first filter (F1). We then applied a second filter (F2), where we read the articles' titles and abstracts, ensuring that they (1) proposed a visualisation or notification method or tool, (2) included strategies for awareness and/or control, (3) described actual design or results, (4) could serve the IoT domain. The criteria were met by twenty-four articles. Finally, we performed paper snowballing and included 19 more articles. In total, we included 42 articles in our survey (23 from our search and 19 from snowballing).

Table 1. Search queries and terms used in acquiring literature

Search queries and terms	
ACM (95 Results)	**IEEE** (48 Results)
(("Abstract":"privacy") AND ("Full Text Only":"web" OR "Full Text Only":"mobile" OR "Full Text Only":"IoT" OR "Full Text Only":"Internet of Things") AND ("Abstract":Visual* OR "Abstract":design*) AND ("Abstract":polic* OR "Abstract":regulation*) AND ("Full Text Only":noti*) AND ("Abstract":aware* OR "Abstract":control*)) **Filter by:** [Publication Date: (01/01/2016 TO 31/12/2022)], [language: English], proceeding, research article.	[Abstract: "privacy"] AND [[All: "web"] OR [All: "mobile"] OR [All: "iot"] OR [All: "internet of things"]] AND [[Abstract: regulation*] OR [Abstract: polic*]] AND [[Abstract: visual*] OR [Abstract: design*]] AND [All: noti*] AND [[All: aware*] OR [All: control*]] **Filter by:** Conferences, 2016 - 2022, English
Science direct (32 Results)	**SpringerLink** (18 Results)
("notice" OR "notify" OR "notification") AND ("web" OR "mobile" OR "IoT" OR "Internet of Things") Title, abstract, keywords ("privacy") AND(("regulation" OR "policy") AND ("visual" OR "visualization" OR "design") AND ("aware" OR "awareness" OR "control") **Filter by:** Research articles, Year: 2016-2022, English	'"polic*" AND "visual*" AND "noti* AND " AND "aware* AND " AND "control*" AND "privacy" AND ("web" OR "mobile" OR "IoT" OR "Internet OR of OR Things")' **Filter by:** English, Conference Paper, 2016 - 2022
Google Scholar initial search (222, 400 Results)	**Google Scholar specific terms search** (6158 Results)
("notice" OR "notify" OR "notification") AND ("web" OR "mobile" OR "IoT" OR "Internet of Things") AND ("privacy") AND ("regulation" OR "policy") AND ("visual" OR "visualization" OR "design") AND ("aware" OR "awareness" OR "control") **Filter by:** 2016 - 2022, no citations, no review articles	("notification" AND "privacy" AND "awareness" AND "control" AND "policy") AND ("visualization" OR "visualisation") AND ("web" OR "mobile" OR "IoT" OR "Internet of Things") **Filter by:** 2016 - 2022, no citations, no review articles

2 USER-CENTERED PRIVACY MANAGEMENT IN THE WEB AND MOBILE ERA

One of the most popular web privacy management protocols is the Platform for Privacy Preferences Project (P3P) [128]. Until it became obsolete, the P3P protocol provided a standardized and machine-readable policy format for websites to express their privacy practices in the form of XML-based privacy policies. The P3P protocol helps ensure informed website practices by specifying four factors that could have an impact on privacy management. These four factors are data categories, purpose, retention, and recipients. Figure 2 depicts the P3P protocol, demonstrating how users can be made aware of how their data is handled.

The P3P protocol has led to the development of numerous web and mobile tools aimed at assisting users in managing their privacy. Some tools used all four of the P3P privacy management factors, while others only used a subset of them. Some have added new factors to assist users in managing their privacy. Below, we discuss these tools and summarize them in Table 2.

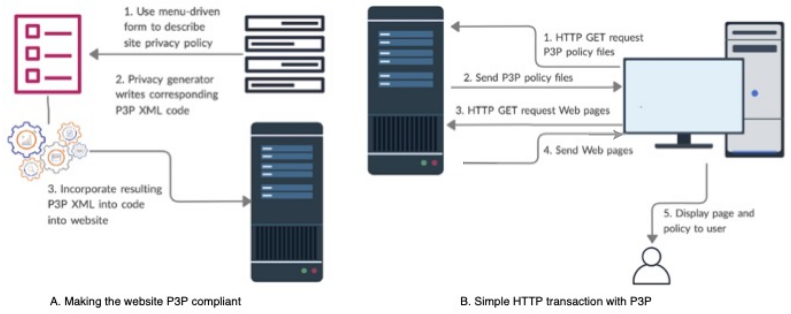

Fig. 2. Basic P3P protocol functionality based on [39], (a) is how to make a website P3P compliant. (b) is a simple HTTP transaction with P3P incorporated.

Browser exertions' have been used to protect users' privacy on the web. *Privacy Bird* [41] uses the P3P language, which allows for the specification of recipients, data categories, purpose, retention, and consequence in one or more privacy statements. *PrivacyCheck* [161] utilizes data mining models to automatically summarize website privacy policies. The summary presented to the user answers ten questions about the type of information obtained, how the information is used, and whether the information is shared. *Privee* [169] employs six classifications to provide a grade of a website's privacy policy. The six classifications are collection, storage encryption, limited retention, ad tracking, profiling, and ad disclosure.

Several other solutions for better communicating privacy policies have also been proposed in research. *Contextual Privacy Policies (CPPs)* [119] display a container that is embedded directly in the context of use and contains what information the websites gather and why. *Nutrition Label for privacy* [83] employs three P3P specifications, namely recipients, data categories, and purpose, and displays them in multiple triplets of information. The *Nutrition label* was expanded by *Visual Interactive Privacy Policy (VIPP)* [130] and *Privacy policy options (PPO)* [108] by adding control options and more data sharing information, such as retention and deleting stored data. *SecFilter* [65] allows organisations to develop policies for information sharing and visualises the volume of consumption and sharing through topic graphs. *PrivOnto* [117] employs a semantic framework to express data practices in privacy policies and visualise them using a web interface. In addition, Schufrin et al. [140] proposed a web-based tool that allows users to interactively explore the temporal aspect of data collected from various online services.

The PrimeLife project [54], which was designed for European privacy laws, contains several prototypes to enhance privacy policies. It includes three privacy concepts: data types, data purpose, and data processing, i.e., storage. As part of the PrimeLife project, Angulo et al. also proposed the *Send data* prototype [11]. The *Send data* prototype specifies three PrimeLife Policy Language (PPL) attributes: data attribute type, purpose, and access credentials. The *Privacy Policy Visualization Model (PPVM)* [62] is also regarded as one of the first attempts to visually represent and improve the usability of privacy policies. The *PPVM* specification specifies five elements that comprise a privacy policy: purpose, visibility, granularity, retention, and constraint. *Privacy Wheel* [153] used clickable wheel spokes to display eight privacy concepts, including collection, data quality, purpose, limited use, security, consent, third parties, and accountability. Other tools, such as *Data Track* [10] show the disclosure of users' data to service providers and address data access stored on the service's side. *Poli-see* [70] extended *Data Track* and addresses data type, data usage, data transformation, data collector and third parties, and any available configuration options. Lomotey et al. [101] proposed *Data Trusts as a Service (DTaaS)*, a cloud-based platform that facilitates data

sharing among multiple partners. *DTaaS* employs visualisations to enable data subjects to see where their data is, control who has access to it, and decides how it can be used.

In addition to web interfaces developed to better communicate the privacy implications [72, 125], research was also proposed to improve the usability of privacy policies in mobile applications. Kelley et al. [84] address the display of mobile application data collection and usage as privacy facts, allowing users to make better privacy decisions. Tian et al. [152] proposed a mobile application hook to help users express their privacy concerns. Chen et al. introduced the *SweetDroid* framework [31], which provides automated privacy policy generation and enforcement and includes information such as data type, purpose, and data access. Paspatis et al. [123] presented *Appaware*, a visual model for representing privacy policies in which it generates visual reports regarding mobile app privacy permissions. Eza et al. [51] created *APPviz*, which visualises how third-party apps use users' data via a tree map, time chat, radar chart, and data map. Bemmann et al. [24] created a mobile privacy dashboard that allows users to view and control their data more transparently.

Sadeh et al. [136] proposed *PEOPLEFINDER*, an application that allows mobile and web users to share their location and specify the duration of the sharing. Ataei et al. [20] designed a mobile user interface that enables users to control their location privacy through three sharing preferences: whom, when, and where. Other research has proposed mobile interfaces that allow users to control the degree of granularity for location [141] or different sensing modalities [35] to give users control over their data and raise their privacy awareness. Christin et al. [34] further extended the mobile interface [35] to include the use of picture-based privacy warnings and the ability for users to configure their privacy settings.

3 USER-CENTERED PRIVACY MANAGEMENT IN THE IOT ERA

Enhancing users' privacy in the IoT domain is a more challenging topic. IoT devices are small in nature and usually get unnoticed. As a result, mobile and web notification solutions may not be appropriate in the IoT environment. Despite the fact that several studies have proposed various interfaces to increase individuals' privacy awareness and control in the IoT, the field of IoT privacy remains limited. Below we discuss several studies that looked into increasing user awareness of data privacy in the IoT domain. A summary of the IoT tools is presented in Table 2.

Feng et al. [52] proposed the *IoT Assistant app (IoTA)*, which provides a summary of the privacy practices for nearby IoT devices and allows users to configure their privacy preferences if they are available. Escher et al. [50] presented a *transparency app* that can notify users about nearby IoT devices and their associated data practices via smartwatches and smartphones. Georgievski et al. [59] suggested using robotic assistance to improve privacy awareness in smart settings, allowing users to build privacy policies using a set of privacy policy rules. Kleek et al. [154] created *IoT Refine*, a privacy visualisation disaggregator that analyses IoT devices' network traffic to visualise their data collection and usage practices. Further, Pardo and Métayer [122] introduced *PILOT*, a privacy policy language that allows data controllers to define specific privacy policies and indicate related privacy risks. Data subjects can also express their privacy consent through *PILOT*.

Gisch et al. [63] proposed the *Privacy Badge*, which visualises four types of data loss: what data was disclosed, when it was disclosed, to whom it was disclosed, and for what purpose the data was disclosed. Gehring and Gisch [58] improved the *Privacy Badge* to give users the ability to configure their privacy preferences. Greene et al. [67] introduced the *ShareHealth* system and proposed a mobile visualisation prototype that enables users to specify access-control policies for their health data. Other studies, such as [164], also discussed giving users control over their data so they can perform their desired privacy configurations.

Fernández et al. [53] visualised and analysed data collected by IoT devices through their *Graph-Based Data-Collection (CBDC)* framework. The *CBDC* framework displays five policy entities namely

Table 2. Main factors influencing privacy management (awareness and control) in web, mobile, and IoT.

Web and Mobile

			Privacy Bird [41]	*PrivacyCheck* [161]	*Privee* [169]	*CPPs* [119]	*Nutrition Label for privacy* [83]	*PrimeLife* [54]	*Send data* [11]	*VIPP* [130]	*PPO* [108]	*SweetDroid* [31]	*Prihook* [152]	*PPVM* [62]	*Data Track* [10]	*Poli-see* [70]	*Privacy Wheel* [153]	*TransparencyVis* [140]	*Privacy Facts* [84]	*Habib et al.*[72]	*Privacy Booklets* [125]	*PEOPLEFINDER* [136]	*Scipioni and Langheinrich* [141]	*Christin et al.* [35]	*Christin et al.* [34]	*SecFilter* [65]	*PrivOnto* [117]	*APPviz* [51]	*Ataei et al.* [20]	*Appaware* [123]	*Bemmann et al.* [24]	*DTaaS* [101]
Privacy Management	Awareness	Data type **(What?)** Defines collected data type.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Data Usage **(How?)** Defines collected data usage purpose and how the data is handled.	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓		✓	✓	✓					✓	✓			✓	✓	✓
		Data Retention **(When?, for how long?)** Defines collected data retention period and collection time.	✓		✓					✓	✓		✓	✓				✓			✓	✓					✓	✓	✓		✓	✓
		Data Storage **(Where?)** Defines collected data storage location and where the data is kept.	✓	✓	✓	✓		✓		✓	✓		✓	✓	✓	✓					✓							✓	✓		✓	✓
		Data Access **(Whom?)** Defines access to the collected data, with whom the data is shared, and to whom the data is transferred. (granularity, transparency, visibility)	✓	✓	✓		✓		✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	control	Provides Control Defines allowing users to perform privacy preferences configuration	✓						✓	✓	✓	✓	✓				✓			✓		✓	✓	✓	✓	✓	✓		✓	✓	✓	✓

IoT

			IoTA [52]	*Robotic Assistance* [59]	*Privacy Badge* [63]	*Enhanced Privacy Badge* [58]	*PatrIoT* [164]	*CBDC* [53]	*Salgado et al.* [44]	*DigiSwitch* [27]	*ShareHealth* [67]	*PILOT* [122]	*IoT Refine* [154]	*Transparency app* [50]
Privacy Management	Awareness	Data type **(What?)**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
		Data Usage **(How?)**	✓		✓	✓	✓	✓	✓			✓	✓	
		Data Retention **(When?, for how long?)**	✓		✓	✓	✓	✓	✓	✓	✓	✓		✓
		Data Storage **(Where?)**	✓				✓	✓	✓			✓	✓	
		Data Access **(Whom?)**	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	control	Provides Control	✓	✓	✓	✓	✓		✓	✓	✓	✓		

device, data items, category, action, and service. Salgado et al, [44] extended the nutrition label through the use of mobile card sorting to control the privacy preferences of smart toys. Caine et al. [27] developed the *DigiSwitch* medical system, which uses a digital photo frame to visualise the collected data and allows users to pause data transmission.

4 PRIVACY MANAGED INFRASTRUCTURE

We presented a summary of the available tools and models designed to provide users with privacy awareness and control in Table 2. We concentrated on the tools and models that help enhance the visualisation of privacy policies and allow users to better understand and control their data. Table 2 shows that most tools focus on addressing five major factors, namely (data type, data usage, data storage, data retention, and data access), while some tools also provide control options to assist users with their privacy management. Most privacy studies have identified these factors as the primary sources of concern for individuals regarding their data privacy [92, 114, 118, 145].

Table 2 shows that the majority of the tools and models were created for the web or mobile, with only a few for the IoT domain. Therefore, the focus of this paper is on mapping the five major factors that play a role in improving users' privacy management to the IoT domain. Each of these factors and how they apply to the Internet of Things is discussed in this section. We also discuss the various notification methods that were used to frame and present the privacy notices to users (such as colour, icons, text, hoovering and pop-up notices) in the next section.

To this end, a privacy notice must address the five main factors in order to raise individual awareness and control of IoT privacy. Figure 3 presents a definition of each privacy management factor. To begin, the user must understand the type of data being collected, such as audio, video, and/or temperature data. Second, the user must recognize data usage, which identifies the purpose of data collection, such as marketing, energy saving, entertainment, security, or other purposes. The user must then know where the data is stored, specifically if it is on the device or in third-party storage. Data retention, which specifies the time and frequency of data collection, is the fourth factor that demands the user's attention. Fifth, the user should know who has access to their data and at what level of granularity and visibility. Finally, and most importantly, an effective notification modality must be used to alert the user to the presence of an IoT sensor in the vicinity.

4.1 Data Type

Data type, as shown in Figure 3, defines the type of data being collected or monitored [92, 118]. Given the heterogeneity of IoT devices, they collect multiple data types to provide services to consumers [124]. Several privacy studies discussed that despite the widespread use of IoT devices, users are often unaware of the data IoT devices collect [74]. For this reason, specifying the types of data collected by an IoT device in a privacy policy is important to give users a clear understanding of what information is collected about them [94].

IoT devices collect various types of data using their embedded sensors [118]. These sensors usually share the collection of common data types that enable them to perform multiple tasks [43, 109]. Table 3 in this section lists some examples of IoT sensors, types of collected data and the relevant IoT applications. The data types and sensors list was generated during our review of available literature, but it is intended to be extensible. While we divided Table 3 into sections, the data tabulated can overlap since IoT devices usually use a combination of sensors and data types. For instance, according to Table 3, a smart thermostat can monitor environmental data, such as temperature and humidity levels, through temperature and humidity sensors [137].

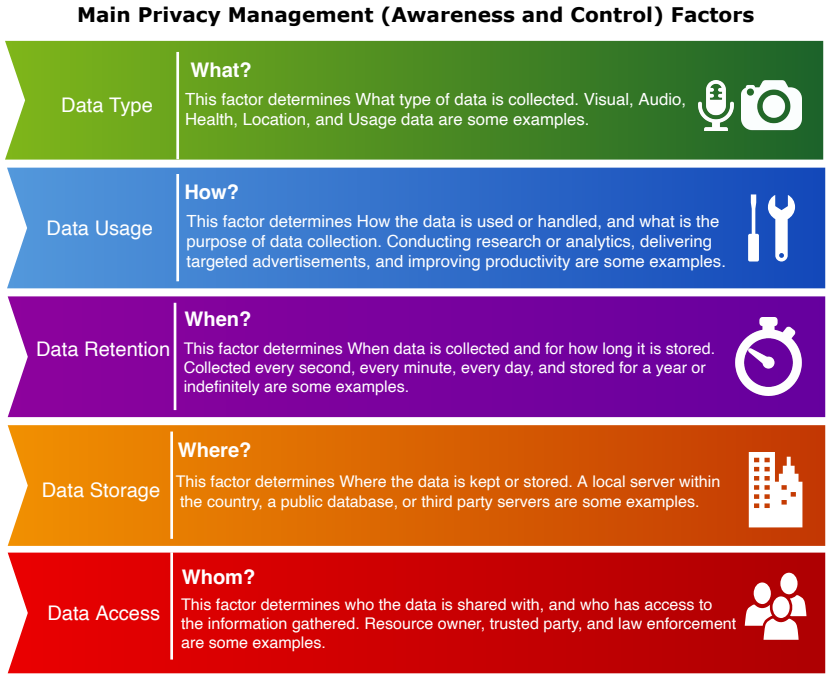

Fig. 3. Main privacy management (awareness and control) factors that must be included in a privacy notice for the user to understand how an IoT sensor collects and processes data.

4.2 Data Usage

Data usage defines the purpose of data collection [2, 118]. In any privacy policy, specifying the purpose is essential since it identifies why data is collected and how it is handled [2, 118]. In the IoT context, data usage purposes vary based on the IoT device and its deployment. Some usage purposes are clearly defined in the privacy policies, while some are contextual and inferred. The following subsections give examples of data usage purposes in the IoT domain.

4.2.1 The primary purpose of data usage. The purpose of using the collected data would be determined primarily by the device that is collecting it. Typically, when a user purchases a specific sensor, the privacy policy attached to the device will specify one or more specific purposes for data usage. That is similar to the web's privacy policies, which users routinely ignore and accept without further investigation.

Table 4 summarizes the main purposes of data usage. We included one IoT device from each section of Table 3 in Table 4 based on the common data usage purposes specified in previous literature [1, 38, 74, 86, 110]. It is important to note that the purposes classified in Table 4 are the abstract purposes defined by the device, which typically do not reveal information about what is done with the data. In order for the device to comply with its standard privacy policy, the data collection purpose must be specified. When presenting the purpose of the data collection, manufacturers frequently use a dim view [36]. For example, a smart smoke detector manufacturer may state in their privacy policy that they are using user data to improve research and analytics, which will help in providing a better user experience. The underlying mechanism, however, is different. Manufacturers track users' activities, such as how frequently and for how long they smoke, how

Table 3. Data types collected by IoT sensors based on [12, 22, 142, 151].

Sensor Type	Data Type Detected	IoT Device Application
• Sound Sensor	• Audio • Ultrasonic waves	• Voice recognition systems • Distance measurements
• Camera Sensor • Colour Sensor • Light Sensor • Fire Sensor	• Images and Video • Lights illumination (colour Photodiodes) • Ultraviolet radiation	• Monitoring systems • Face recognition systems • Smart lighting systems
• Smoke Sensor • Gas Sensor • Odour Sensors	• Smoke and Gas • Oxygen and carbon dioxide levels • Infrared signals	• Air quality monitoring • Smoke detection systems • Smart Gardening
• Level Sensor • Temperature Sensor • Alcohol Sensor • Moisture Sensor	• Temperature level • Oral data • Breath	• Alcohol monitoring systems • Diet monitoring systems • Food tasting systems
• Touch Sensor – Force Sensor • Skin Sensor • Electromyography • Proximity Sensor • Vibration Sensor • Line Finder • Distance Sensor	• Biometrics • Pressure applied • Skin's electrical conductivity • Magnetic forces • Body temperature • Body movement • Capacitance change • Infrared signals • Orientation • Impact	• Fingerprint scanner • Galvanic skin response • Medical systems • Security systems • Smart toys • Smart appliances • Vehicles seat monitors • Smart vacuum • Activity trackers • Smart transportation • Smart locks
• Heart rate Sensor • Optical Sensor • Gesture Sensor • Rotary Sensor • Motion Sensor – Gyroscope – Accelerometer – Magnetometer	• Blood movement • Muscles Signal • Velocity (Speed) • Acceleration • Proximity • Presence • Infrared Signals • Rotation (direction)	• Sleep monitors • Heart-rate monitors • Wearable sensors • Baby monitors • Blood sugar monitor • Transponders on animal • DNA analysis devices • Smart navigation systems
• Humidity Sensor • Water Sensor • Turbidity Sensor • Ultraviolet Sensor • Dust Sensor	• Humidity level • Atmosphere pressure • Slop • Dissolved solids • Hydrogen ion • Dust concentration	• Tank systems • Sewage systems • Liquid sensing applications • Pharmaceuticals • Dyeing process • Smart meter • Smart thermostat

many people smoke, whether the smoke comes from a cigarette or another burning object, etc. Such data collection purposes are typically not covered by a privacy policy [36]. This information is commonly referred to as inferred knowledge of the data collection purpose, which is further discussed in the subsection that follows.

4.2.2 The secondary purpose of data usage. As previously stated, the goal of using the collected data extends beyond the abstract concept of improving research, and analytics [121]. It, on the other hand, spans a much wider area [149]. The more data the device collects, the more knowledge it will have and be able to build [60]. The accumulation of this knowledge has the potential to

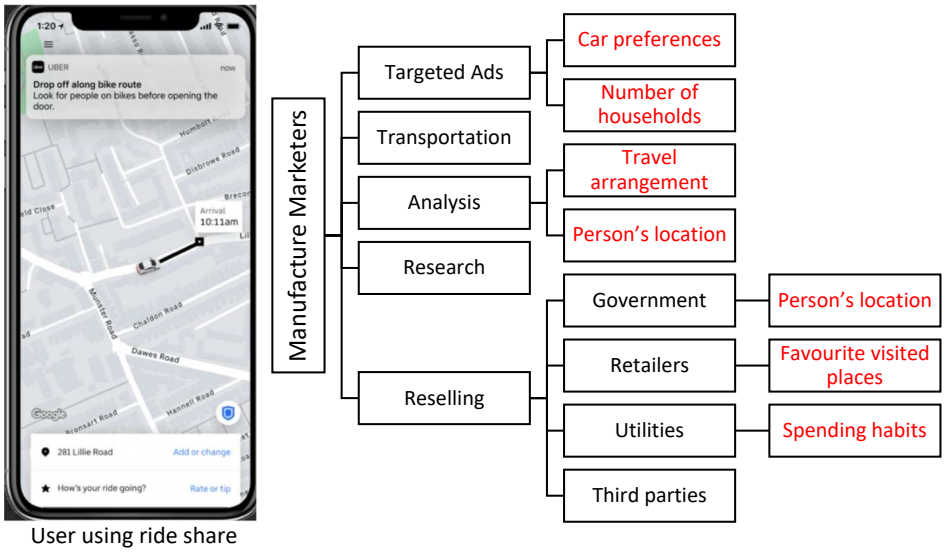

Fig. 4. An example of a ride-sharing application demonstrating how additional knowledge can be derived from the specified data usage purposes. The red boxes represent inferred knowledge, and the black boxes represent the privacy policy-specified data usage purposes.

lead to the creation of a complete human profile [133]. Figure 4 shows how inferred knowledge can be derived from a simple ride-sharing application. Consider the following scenario to describe the value of the collected data, which show how the inferred knowledge could benefit service providers while also affecting individuals' data privacy.

1) Monitoring systems: This section presents a fictional use case scenario about a company called Visa. Sara needs continuous monitoring of her home due to her frequent travel. Visa is a useful IoT monitoring system that provides users with a motion-detection camera to monitor their homes easily. The camera has multiple sensors (e.g., sound, camera, motion) to collect data. The camera sensors process the user's personal data, such as audio, images, video, and presence data, whenever motion is detected. The sensors then wirelessly transmit the collected data to the service provider's [1] local or remote cloud servers. Visa keeps its users' camera recordings for as long as their accounts are active or for the legal retention period. Visa users can grant others access to view their camera recordings. The service provider can perform advanced analysis of the users' data in the cloud to improve their services and suggest users with different security monitoring plans. The service provider could also archive recordings in the cloud or share the data with third parties to enhance security monitoring.

Given the above scenario, Sara's camera recordings pass through various nodes until they reach the application that allows her to monitor her camera remotely. These nodes include, but are not limited to, third-party network providers, third-party storage services, and third-party service providers. One or more of these nodes may sell or share Sara's data with third parties for analytical purposes. Figure 5 depicts Sara's thoughts about her data usage and the actual data usage. The data collected by the security monitoring camera can be used to infer sleeping habits, travel habits, the number of visitors, the number of occupants in a specific area, and much more. In 2019, Amazon Ring video doorbell announced that the videos recorded on their "Neighbors" app are

[1]The terms Visa and service provider are used interchangeably in this scenario

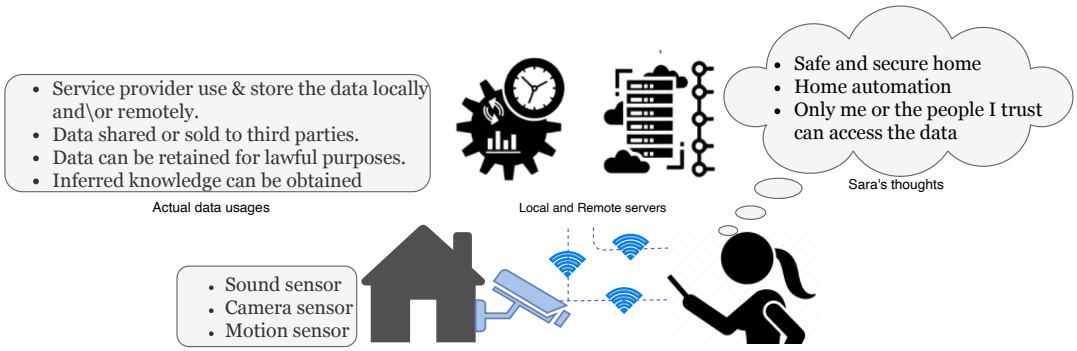

Fig. 5. A monitoring system data usage use case scenario includes the user's expected data processing as well as the actual data processing.

used by at least 400 law enforcement agencies nationwide to aid in criminal investigations [150]. Ring video doorbell is an IoT device that is installed in front of a person's home. It continuously detects motion and records videos, allowing users to communicate with people passing by their property via audio and video [132]. The "Neighbors" app also provides users with real-time safety alerts from the local police department and residents in the same neighbourhood [132]. Although the Ring app allows users to choose whether or not to share their videos with authorities, there were many privacy concerns about the knowledge that can be inferred from the collected data. Concerns have been raised that the inferred knowledge could enable the police to obtain an official search warrant requesting an individual's videos [112].

4.3 Data Storage

Storage of data refers to the place where the collected IoT data is kept. In the context of IoT, a single IoT device may rely on multiple sensors to provide a service, with each sensor requiring a unique type and format of data [21]. The collected data will then be stored in a storage location(s) to be processed [163]. Storage locations differ depending on the IoT device, its manufacturer, and the service it provides [120, 166].

Given IoT devices reduced hardware capabilities and the need to collect data continuously [21, 71], many organisations are storing the data in the cloud [163]. For example, medical, surveillance, energy, and other data collected by IoT sensors are stored in the cloud [12, 90]. While storing IoT data in the cloud has benefits, such as data analysis and classifications, outsourcing data to the cloud introduces privacy risks and can lead to losing control over the device [71, 98]. Researchers suggest implementing access control mechanisms to secure cloud data [71, 98].

In addition to access control, it is imperative that the privacy policies of IoT devices specify where data is stored. Doing so will notify users about where their data is and whether the specified location complies with their country's same privacy rules [98]. Data protection rules differ in different jurisdictions, so storing data in a jurisdiction other than where the data was generated can pose additional privacy risks [13, 99]. In Table 4, we list examples of the possible data storage locations based on literature [9, 33, 71, 99]. According to Table 4, smart thermostat data might store the collected data in a third-party server to improve analytics.

Table 4. A sample of IoT devices collected data usage purposes, storage locations, retention period, and accessing entities.

IoT Device Application	Purpose	Storage Location	Retention Period	Accessing Entity
• Voice recognition systems • Smart lightning systems • Smoke detection system • Food tasting system • Security systems • Heart-rate monitors • Smart thermostat	• Revenue • Productivity • Research • Analytic • Statistics • Security • Safety • Health • Surveillance • Targeted Ads	• Local Server • Remote Server • Third-Party Server • Public Server	• Indefinite • Stated period: i.e., Weeks, Months, or Years • Until purpose(s) met • Legal retention: i.e., legal retention is required	• Resource Owner • Trusted Party • Service Provider • Device Manufacturer • Law Enforcement • Third Party • Marketing organisations

4.4 Data Retention

The term data retention describes how long a data collector keeps the collected data in their database [118]. Data retention is a critical component of privacy policies. As shown in Figure 6, in addition to specifying the purpose of data collection, privacy policies on websites typically mention data retention. Defining how long data should be retained in an IoT privacy policy can depend on several factors [118]. First, IoT devices typically have multiple sensors, each requiring a different retention period [21]. Second, IoT devices have different memory sizes, application requirements, bandwidth, and throughput, resulting in a variation in the required retention period [29].

Retention period has a significant impact on users' willingness to share their data [95, 110, 115]. According to [110], when it comes to data retention, most people prefer devices with a short retention period or the option of data deletion. Leon et al. [95] also noted that when users were informed that the retention period would exceed a week, they were less likely to share their data [95]. Table 4 tabulated multiple retention period options mentioned in previous literature [56, 81, 105, 110, 118].

4.5 Data Access

The context for data access is an important factor that has been considered in almost every privacy policy. Data access specifies who has access to and shares the collected data. In the IoT domain, data access is crucial, and with the big data generated by IoT devices, many entities can access data. IoT manufacturers often work with third parties to obtain the necessary facilities for improving their service and conducting their IoT operations. This implies that users' data will potentially be made available to more entities than the data owner would anticipate [107]. These entities may adhere to the same privacy policy the IoT service provider follows or even have their own privacy practices. While some entities' privacy policies clearly state that they do not sell or share the collected data, others state that they do. Data is frequently shared with third parties to enhance service; however, data may be shared with other parties in response to a legal order. Furthermore, data can be accessed for a variety of other purposes, including fulfilling user requests and preventing illegal activity such as fraud.

It is critical that users understand who has access to their data. Data owners should be able to choose whether or not to share their data with entities regarding an operation and a purpose. The data owner must also control how detailed the data provided in response to a specific access request is. For example, a patient must be able to restrict access to their medical data to only their family physician and not a third party, such as a future potential insurance company. Furthermore, data owners should be able to control when their data is accessed. For instance, several mobile platforms

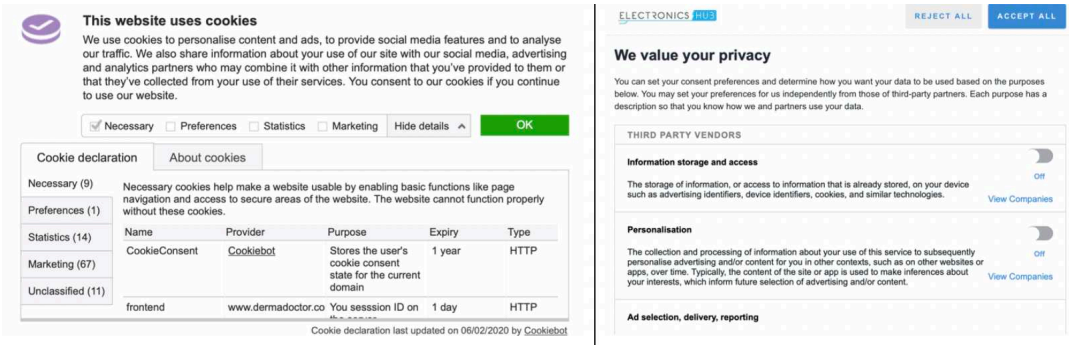

Fig. 6. A sample of two websites' privacy policies, with which the user must agree to browse the selected website [45, 76].

provide users multiple options for an app's access to location data acquired by the device, such as "always," "when using the app," "never," and "only once."

Table 4 presents a selection of entities that may have access to individuals' data based on the common data access specified in previous literature [1, 38, 74, 86, 110]. According to Table 4, trusted parties, such as medical professionals, might have access to data collected by heart-rate monitors in order to improve user productivity.

5 NOTIFICATION METHODS

As stated in the introduction, existing notices fall short of providing users with the required IoT privacy knowledge. The importance of the notification mechanism stems from the widespread proliferation of IoT devices, which have become deeply embedded in daily life that they go unnoticed by people [46]. In this section, we provide a comprehensive survey of the notification methods. The goal is to provide a toolkit that presents the various available techniques as a foundation for future studies and research.

We present several works of literature that have investigated notification methods in different contexts in the following two subsections (Section 5.1 and Section 5.2). Some notification methods have been used in the design of privacy notice and/or control solutions, as discussed in Section 2 and Section 3, while others have been used to deliver other types of notice and/or control. We categorise the research papers into a three-step design pattern in Section 5.1 (presentation, framing, and interaction). In Section 5.2, we create a privacy management design toolkit (see Figure 11 (i)) and present a use case example and two examples from the literature on how to apply the toolkit. Through this, our goal is to provide developers and future researchers with a research foundation and toolkit for creating effective IoT privacy notices that improve user privacy management (awareness and control).

5.1 Presentation, Framing, and Interaction

Following the identification of the five major privacy factors for IoT devices' privacy notice, these factors must be effectively delivered to the user. Several studies have found that effective privacy notice allows users to understand the privacy subject better and be more informed about their data, allowing them to make better privacy decisions [25, 77, 126]. During our survey, we distinguished that the majority of the literature enhancements to privacy notice visualisations follow a three-step design, (i) presentation, (ii) framing, and (iii) interaction, as shown in Figure 11 (i). We used the three-step design pattern to categorise prior work notification methods in Table 5.

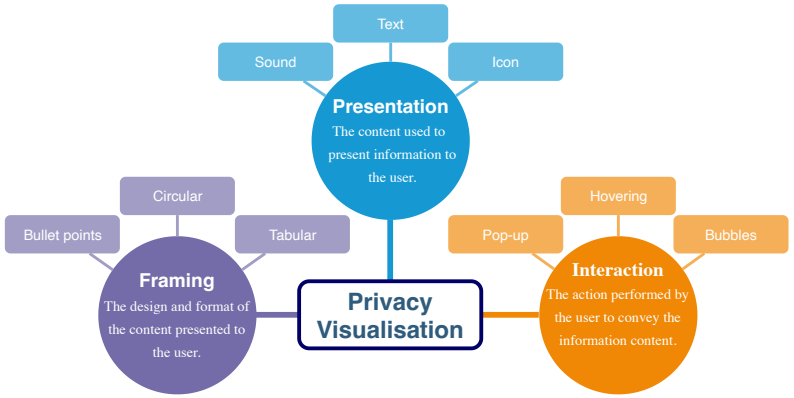

Fig. 7. Privacy visualisations categorised into a three-step design pattern. Each category has a wide range of application contexts.

To effectively deliver a privacy notice to the user, literature used various forms of presentation, such as icons or text. Some literature used different framing techniques, such as changing the colours and intensity to encourage users to read the privacy notices. Furthermore, in the literature, some forms of interaction, such as bubbles and hovering, have been used to engage users in interacting with privacy notices. Figure 7 presents a definition of the three-step design pattern for providing users with privacy information. Because the three-step design pattern components overlap, each of the three subsections that follow may contain information that applies to the other subsection. We present the literature and describe the format they used to present an effective notice in the following subsections.

5.1.1 ***Presentation.*** Presentation is defined as the content used to present information to the user. In the context of privacy, this content could include icons, text, nods, sounds, and other elements (refer to Figure 11 (i)). This section provides a brief overview of presentation in literature. Some of the literature was not privacy-specific but used presentation content (see Table 5).

Privacy Bird [41] uses a bird icon with changing colours, speech bubbles, and noises to notify users whether the privacy policy of the visited website matches their privacy preferences. *The PrimeLife project* [54] initial proposal includes 30 icons that comply with European privacy laws. Their user studies confirmed that the presentation of privacy policy icons must be simple and neutral. Figure 8 (iii) displays the icons that received the highest ratings during their evaluation. These icons are what we refer to as one of the presentation content. *PrivacyCheck* [161] summarize web privacy policies and display them as changing colour graphical icons. Further, *Privee* [169] used text and coloured rating to summarize the privacy policies and indicate the level of privacy risk of how data is handled, refer to Figure 8 (I). *Ataei et al.* [20] created a user interface that allows the users to manage location privacy through three main circular icons. *Appaware* [123] used representative image to visualise Android apps permissions. *DTaaS* [101] used an icicle tree with text and multiple colours visualisations to allow users to track their data workflow.

Research has also looked into improving the presentation of privacy information in mobile [84, 164] and web interfaces [72, 125] to better communicate the privacy information. Sadeh et al. [136] proposed mobile and web interfaces with notification bubbles, explanation functionality, and auditing feature to enhance users' understanding of their privacy policies. Feng et al. [52] introduced the *IoT Assistant app (IoTA)*, which employed a map view and coloured icons with texts to visualise the data collected by nearby IoT devices. Gisch et al. [63] proposed the *Privacy Badge*,

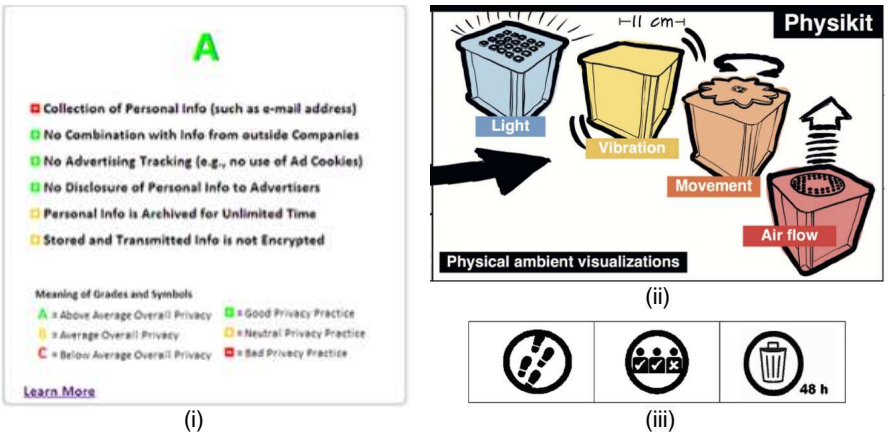

Fig. 8. Example from the literature of the presentation step content: (i) Text and Rating to visualise the privacy Policies [169], (ii) Tangible objects to visualise the sensed data [75], (iii) The most popular icons from the PrimeLife project [54]

which visualises data loss and privacy preferences with colours, icons, and bubbles. Gehring and Gisch [58] used icons, colours, and pop-ups to improve the *Privacy Badge* and give users control over their data. Sliders, icons, and various colours were used in [35, 141] to provide mobile users control over their data. Furthermore, Christin et al. [34] incorporate images with different colours in the privacy notifications to raise users' privacy awareness. The authors of [25] discussed displaying a small notification at the top of the screen to reduce the users' annoyance when they receive a call.

Several studies have also looked into the use of sounds to notify users, whether in the privacy or non-privacy domain. M. Haslgrubler et al. [73] used audio notifications to alert industrial workers of potential hazards. Chernyshov G., et al. [32] used melodic rhythm as an audio notification approach to help users understand the status of an IoT device. The sound of push notifications in smartphones and Amazon Alexa is perceived as an audio notification that informs users about an event or the use of their data [89].

Multiple efforts used tangible objects to notify users and capture their interest in noticing the collection and processing of their data. Houben et al. [75] proposed using tangible cubes that emit light, vibrate, or heat up to inform users about the use of their data. Figure 8 (ii) depicts the cubes used to visualise the sensed data. These tangible objects are what we refer to as one of the presentation content. Georgievski et al. [59] used tangible robotic assistance to view a brief text user-defined privacy policies, which can enhance users' privacy awareness in smart settings. The tangible approach has also been used as an effective method of notification and interaction in [14, 88]. *IoT Refine* [154] visualised data flow to increase smart home users' awareness through an ambient display with varying text and colours.

5.1.2 ***Framing.*** While presentation refers to the content of the privacy policy or notice, framing refers to how that content can be structured and designed to be presented and delivered to the user. Framing can take various shapes and formats. In the context of privacy, some framing formats include using a grid or a circular view; see Framing in Figure 11 (i). Framing can also be achieved by changing the colour, intensity, and/or frequency of the presentation content. This section provides

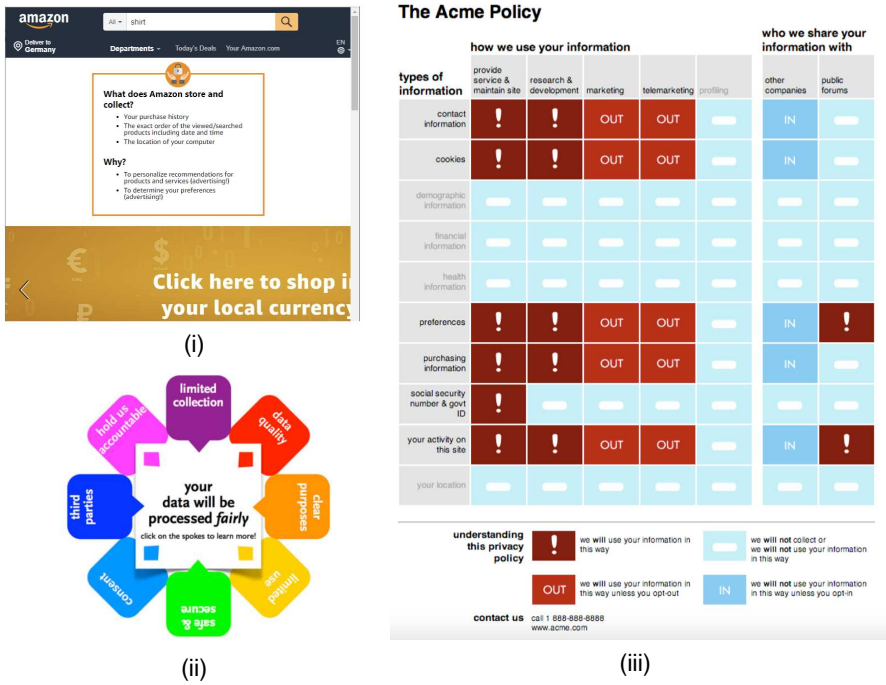

Fig. 9. Example from the literature of the framing step: (i) *CPPs* used Text from the presentation step with framing as Bold, Bullet points, and displaying the privacy policy in the context of use [119], (ii) *Privacy Wheel* used coloured Wheel framing with Text from the presentation step [153], (iii) *Nutrition Label for privacy* used coloured Tabular framing with Text and Punctuation marks from the presentation step [83].

a brief overview of framing in literature. Some of the literature was not privacy-specific, but it used the framing concept (see Table 5).

Several studies used a grid or tabular view to visualise privacy policies for web and mobile applications. Using a variety of colours and punctuation marks, *Nutrition Label for privacy* [83] displays the collected data and how it is processed in rows and columns. Figure 9 (iii) depicts the use of text and punctuation marks from the presentation step in a coloured tabular framing to visually represent the privacy policies. *Send data* [11], *Visual Interactive Privacy Policy (VIPP)* [130], and *Privacy policy options (PPO)* [108] extended the Nutrition label by adding interactive and control elements to the grid cells. *privacy label* [48] presented privacy and security practices using rows and columns to encourage individuals to incorporate privacy and security in their IoT buying decisions. *DigiSwitch* [27] proposed a digital photo frame to visualise the collected data using different colours, buttons, and icons. Mobile applications used a similar view to provide automatic privacy configuration [31], or assist users in expressing their privacy concerns [152]. In addition, Salgado et al, [44] reshaped the nutrition label from a tabular interface into multiple single-linear interfaces and used four switches to provide mobile users with a more convenient way to configure their privacy preferences.

Various research used circular or wheel framing to visualise web privacy policies in a more concise graphical representation. *Data Track* [10] and *Poli-see* [70], used coloured nodes to represent data flow in privacy policy visualisations. By hovering over the nodes, users can learn more about the data and perform configuration if applicable. *Privacy Wheel* [153] used a wheel framing to display eight privacy concepts. Figure 9 (ii) demonstrates the use of text from the presentation step in

a coloured wheel framing to visually assist users in understating the usage of their data. Furthermore, Schufrin et al. [140] proposed a web-based tool called *TransparencyVis* that allows users to visually and interactively explore the collected data. Ghazinour et al. [62] presented a model for privacy policy visualisation *PPVM* using a house symbol and multiple nodes. Fernández et al. [53] visualised and analysed data collected by IoT devices using graphs.

Notification intensity and duration have also been used in studies to deliver task-relevant notifications at the appropriate time and mode [158]. Olalera I. et al. [116], proposed the use of different intensities of vibration signals to notify users of a machine fault. In [75], the authors examined the use of an object that can be placed over a vibrated cube, in which the user will understand the notification based on the direction of the object. Emsenhuber and Ferscha [49] discussed how the intensities of odours emitted by humans or other entities convey information that can be detected using available sensors such as gas sensors or electronic noses. *PILOT* [122] introduced the use of coloured forms to help data subjects visualise the potential privacy settings risks. *Contextual Privacy Policies (CPPs)* [119] displayed a container containing a brief description of the websites' privacy policies in the form of bullet-point lists that are closely related to the context of use. Figure 9 (i) shows how to present main data practices within the context of use by using text with bold and bullet points framing. Similarly, the authors of [40] used a machine-learning algorithm to manage the notification based on the context and the user habit. Their system design is capable of determining the person receiving the notification, the device, the ideal time, and the ideal mode.

Categorisation was also used to create more usable privacy policy visualisations. *PrivOnto* [117] used coloured annotation to assist in mapping the data practices text to its suitable categories and attributes. *SecFilter* [65] categorised the visualisation of sensitive information using topic graphs with coloured nodes. *APPviz* [51] visualised data using four different visualisations and provided the user with the ability to categorise how to view the information. The four visualisations in *APPviz*, each have multiple presentation, framing, and interaction contents, such as nodes, colours, bullet points, and cursor hovering [51].

5.1.3 ***Interaction.*** Interaction is defined as a feature that necessitates individual action in order to convey information. Interaction in the context of privacy policies and notices could allow users to specify their privacy preferences and, if applicable, receive feedback. Some examples of interaction include the user clicking to get a pop-up, the user hovering to get more information, the user selecting from multiple options, etc; see Figure 11 (i) for more examples. We provide a brief overview of interaction in literature in this section. Some of the literature was not privacy-specific, but it did use interaction in its design (see Table 5).

Several studies have discussed the significance of embedding the interaction feature while developing a user notice. To convey privacy information, *Privacy Bird* [41] employs a coloured bird icon with sounds. Users can access and configure their privacy preferences by clicking on the bird icon, as shown in Figure 10 (iii). The *Privacy Badge* [58] has been improved to include pop-ups with a mix of binary and enforced options to allow users to configure their privacy preferences. Pop-ups with sliders were used as a form of interaction by Christin et al. [35] to allow users to control the degree of granularity of their data. Privacy dashboards with pop-ups, icons, and toggles have been used by Bemmann et al. [24] to offer transparency and control for users' data. *Transparency app* [50] employed the use of coloured icons and text to provide users with quick visualised notifications of nearby devices that are collecting privacy information. Sadeh et al. [136] *PEOPLEFINDER* application employed auditing functionality with users' feedback and notification bubbles to interact with users and notify them of any incoming queries, as shown in Figure 10 (ii).

Toggles, switches, sliders, hovering, and clickable icons were used in several other studies to provide user interaction. *Visual Interactive Privacy Policy (VIPP)* [130] added toggles and hovering

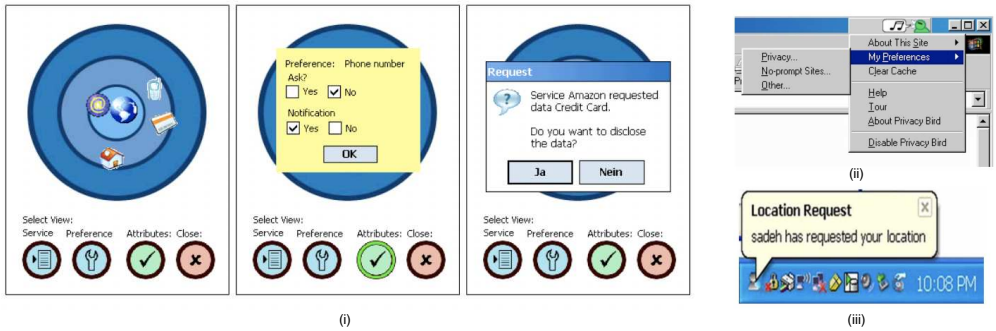

Fig. 10. Examples of the interaction step from the literature: (i) *Privacy Badge* used coloured circular framing with clickable icons and pop-up preferences interaction [58], (ii) *Privacy Bird* Bird used a coloured bird icon and allows users to specify their privacy preferences [41], (iii) *PEOPLEFINDER* displays text in a pop-up bubble to increase user awareness [136].

for users to configure their privacy choices. *Poli-see* [70] added a hovering interaction feature that conveys configuration and privacy information to the user. Salgado et al. [44] reformed *Nutrition label for privacy* symbols into coloured switches to simplify configuring privacy preferences for mobile users. *ShareHealth* [67] employed the use of multiple choices and coloured sliders to allow data owners to define access control policy. Furthermore, according to Habib et al. [72], toggle icons with privacy options assist users in controlling their privacy preferences. As shown in Figure 10 (i) the *Privacy Badge* [58] has coloured clickable icons that provide users with binary and enforced choices to configure their privacy preferences.

On-body interactions, in which a person performs a body action or movement such as smiling or blinking, have also been used as an interaction and feedback option to help with privacy choices [104, 106, 146]. Mehta et al. [106] presented a privacy band that uses an on-body haptic interaction to send notifications to the user. Based on the notification, the band allows the user to respond by submitting feedback, which includes their privacy preferences.

5.2 Privacy visualisation management toolkit

In this section, we present the privacy visualisation management toolkit, see Figure 11 (i). We also provide three examples of how to use the toolkit (Figure 11 (ii)), two from existing literature, (Figure 11 (A) and (B)), and one we developed (Figure 11 (C)) based on the *Monitoring systems* use case scenario described in Section 4.2.2. Each example is denoted by a letter (i.e., A, B, or C), which is then used to represent which items the examples used from the toolkit. We define the toolkit as a knowledge base that synthesizes the key privacy elements identified in prior research. Based on previous research, the knowledge base incorporates not only the most significant privacy notice factors but also how they can be visualised for users. The toolkit is divided into two sections. The first section, on the left, lists the five major privacy factors identified in Section 4. Based on the literature reviewed in this paper, these were the primary factors that should be included in any privacy notice or policy. The second section, on the right, presents a three-step design pattern (presentation, framing, and interaction) identified in Section 5.1 for two privacy concepts (awareness and control). These were the most common privacy notification visualisation methods used in existing privacy notices and/or policies, according to the literature reviewed in this paper. The toolkit demonstrates that privacy awareness is usually required in order to design privacy control.

A future developer can use the toolkit to create a privacy notice for the IoT domain. The content of the privacy notice should address the five major privacy factors. The developer can choose how

Table 5. Pieces of literature presenting the notification methods visualisation; the methods are divided into three categories, each with a unique format.

		Notification Method																												
		Presentation								Framing																Interaction				
Article	Privacy-related	Icon	Text	Arrow	Node	Punctuation	Score	Sound	Sensory	Physical	Tabular	Circular	Map	Label	Bullet-points	Data flow	Category	Bold, Italic, Underline	colour	Intensity	Frequency	Duration	Pop-up	Bubbles	Hovering
Privacy Bird [41]	✓	✓	✓					✓											✓					✓	
PrimeLife [54]	✓	✓																							
PrivacyCheck [161]	✓	✓																	✓						✓
Privee [169]	✓		✓				✓												✓						
Privacy Facts [84]	✓		✓														✓		✓	✓					
PatrIoT [164]	✓		✓																✓	✓					
Habib et al. [72]	✓	✓	✓																✓						
Privacy Booklets [125]	✓		✓							✓							✓	✓	✓						
PEOPLEFINDER [136]	✓		✓															✓	✓				✓	✓	
IoTA [52]	✓	✓	✓																✓						
Privacy Badge [63]	✓	✓	✓																✓					✓	
Enhanced Privacy Badge [58]	✓	✓	✓									✓							✓	✓			✓		
Scipioni and Langheinrich [141]	✓	✓	✓																✓						
Christin et al. [35]	✓	✓	✓	✓	✓														✓	✓			✓		
Christin et al. [34]	✓	✓	✓		✓														✓	✓					
Böhmer et al. [25]		✓	✓																✓			✓	✓		
Haslgrübler et al. [73]								✓											✓						
Ambient Rhythm [32]								✓																	
Kubitza et al. [89]								✓		✓															
Physikit [75]		✓	✓	✓	✓					✓							✓		✓	✓					
Robotic Assistance [59]	✓		✓							✓															
Ardito et al. [14]		✓	✓							✓									✓				✓		
PPVM [62]	✓		✓		✓												✓								
Cubble [88]			✓							✓									✓						
Privacy itch and scratch [106]	✓								✓	✓										✓	✓	✓			
Nutrition Label for privacy [83]	✓		✓			✓					✓								✓	✓					
Send data [11]	✓	✓	✓								✓								✓						
VIPP [130]	✓	✓	✓								✓								✓	✓			✓		✓
PPO [108]	✓	✓	✓								✓								✓	✓					✓
Privacy label [48]	✓		✓				✓				✓			✓					✓						
DigiSwitch [27]	✓	✓	✓							✓	✓								✓	✓			✓		
SweetDroid [31]	✓	✓	✓																✓				✓		
Prihook [152]	✓		✓																✓						
Salgado et al. [44]	✓	✓	✓																✓	✓					
CBDC [53]	✓		✓		✓											✓	✓								
Data Track [10]	✓	✓	✓		✓											✓			✓						✓
Poli-see [70]	✓	✓	✓	✓	✓							✓						✓	✓	✓			✓		✓
Privacy Wheel [153]	✓		✓									✓							✓						
TransparencyVis [140]	✓		✓																✓						✓
Fernández et al. [53]	✓		✓		✓											✓									
Wolpert et al. [158]																				✓		✓			
Olalera I. et al. [116]																				✓					
Emsenhuber and Ferscha [49]																				✓		✓			
CPPs [119]	✓		✓												✓			✓				✓			
Corno et al. [40]																						✓			
SecFilter [65]	✓				✓								✓				✓		✓						✓
PrivOnto [117]	✓		✓														✓	✓	✓						✓
APPviz [51]	✓		✓		✓								✓		✓		✓	✓	✓						✓
Ataei et al. [20]	✓	✓	✓									✓							✓						
Appaware [123]	✓	✓	✓																						
Bemmann et al. [24]	✓	✓	✓												✓			✓	✓				✓		
DTaaS [101]	✓		✓													✓			✓						
ShareHealth [67]	✓		✓																✓						
PILOT [122]	✓		✓												✓				✓						
IoT Refine [154]	✓		✓							✓						✓			✓	✓					
Transparency app [50]	✓	✓	✓																✓				✓		

to present each factor, such as using icons, text, sound, etc. The developer would then decide how to frame the privacy notice and deliver it to the users. Lastly, the developer can incorporate some forms of interactions, such as hovering and/or pop-ups. Below we describe three examples of how to use the privacy visualisation management toolkit.

5.2.1 Visual Interactive Privacy Policy (VIPP). Developed by Reinhardt et al. as a visual interactive privacy policy based on the *Nutrition Label for privacy* [83] and enhanced with control and interactive features [130]. VIPP was designed to introduce transparency and improve user performance and experience while interacting with privy policies. Following the privacy visualisation management toolkit, VIPP (see Figure 11 (A)) can be described as follows:

- **Privacy notice factors:** Data type, data usage, and data access were specified in the title rows and columns. Data retention and data storage were specified in the table through clickable cell interaction.
- **Presentation:** The authors used a combination of text and icons to simplify the presentation of the privacy information. The authors further used toggle switches to offer users privacy control.
- **Framing:** The authors used a tabular format with different colours (orange, blue, and grey), different intensities, and coloured toggle switches to frame the privacy information.
- **Interaction:** The authors used multiple interactive elements, such as mouse-over help icons, expandable rows, clickable cells, and binary and multiple choices toggle switches for consent options.

5.2.2 Poli-see. Developed by Guo et al. as an interactive tool for visualizing privacy policies [70]. Poli-see was created to investigate the extent to which a graphical representation can convey web data use practices and encourage users to engage with their data. Following the privacy visualisation management toolkit, Poli-see (see Figure 11 (B)) can be described as follows:

- **Privacy notice factors:** Data storage and data access were specified as concentric circles. Data type was specified as icons in the inner circle. Data usage was specified via a pop-up sidebar that appears when a user hovers over a node.
- **Presentation:** The authors used a combination of text, icon nodes, and arrows to simplify the presentation of the privacy information.
- **Framing:** The authors used a circular shape with different colours, different intensities and bold text to frame the privacy information.
- **Interaction:** The authors used hovering over some nodes as an interactive feature to convey more privacy information to the users.

5.2.3 Visa. This example aims at guiding developers by demonstrating how to apply the privacy visualisation toolkit for the IoT scenario presented in Section 4.2.2 and shown in Figure 5. As this IoT solution collects personal data that could cause a risk to the user's privacy, it is imperative to provide the user with an effective privacy notice to increase their awareness. To highlight the potential of this, the following example will demonstrate mapping the toolkit to the scenario.

(1) **Privacy Notice five main factors:** The toolkit presented in Figure 11 (i) depicts that a privacy notice should ideally address five privacy factors. Given this scenario, the sensors start collecting different data types when the camera detects motion. **The collected data types are audio, images and video, and presence data.** While other data may be collected, this scenario only considers these data. The collected data are then processed, and **used to conduct analysis, enhance security monitoring, and provide personalised Ads.** The scenario describes that **users' data can be stored in the service provider's local or remote servers. Third parties**

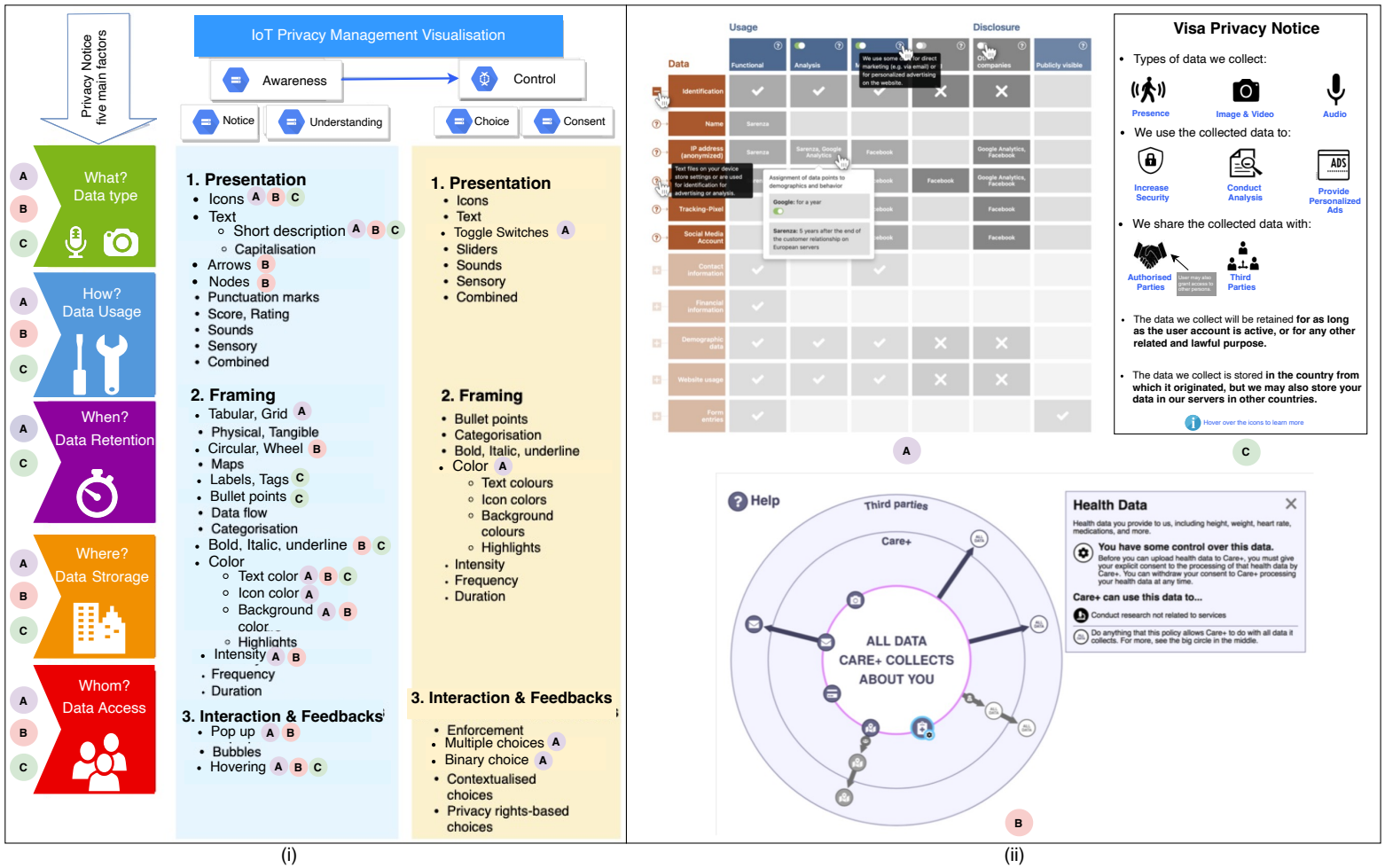

Fig. 11. The left side (i) shows a privacy management (awareness and control) toolkit that can be used to create IoT privacy notices, while the right side (ii) shows three applications of the toolkit. (A) *VIPP* is an example from the literature that used a combination of text, icons, and toggle switches from the presentation step with multiple intensity coloured tabular framing and hovering, pop-up, multiple choices, and binary choice interactive elements [130], (B) *Poli-see* is an example from the literature that used a combination of text, icons, arrows, and nodes from the presentation step with multiple intensity coloured circular framing and hovering and pop up interactive elements [70], (C) *Visa* is a use case example that we developed which used a combination of text and icons from the presentation step with coloured, bold text and bullet point label framing and hovering interactive elements.

and people authorized by the user can access the data. Lastly, the scenario describes that **the data may be retained while the user's account is active or for a legal retention period.**

(2) **Awareness. (2.1) Presentation:** After identifying the factors, we followed by using the toolkit Awareness part. We opted not to use the Control part as the goal was to demonstrate the toolkit application, which can be demonstrated using the Awareness part. We further showed how the Control part is used through the example in Section 5.2.1. Having identified the factors, we selected to present them using **icons and short description text** (refer to Figure 11 (i). We used the examples in Tables 3 and 4 to present the short text for this scenario. We adopted some icons from [4] to visualise the short text.

(2) **Awareness. (2.2) Framing:** After identifying the privacy notice factors and the presentation contents, we framed the privacy notice using **bullet points with bold text, similar to [119], label framing, adopted from [48], and coloured text.**

(2) **Awareness. (2.3) Interaction:** Following the toolkit, we also added a **hovering** interaction element to our privacy notice visualisation. As you can see in Figure 11 (C), hovering over the icons pride uses with an interactive item to increase their awareness.

The resulting visualisation is presented in Figure 11 (C) and can be described as follows:

Visa. Presented in Figure 11 (C) as an example of using the privacy management toolkit for visualizing the *Monitoring systems* scenario privacy policy presented in Section 4.2.2. Visa privacy notice was created to show the application of the privacy visualisation management toolkit and demonstrate that the toolkit can provide new paths for the advance of state of the art. Following the privacy visualisation management toolkit, Visa (see Figure 11 (C)) can be described as follows:

- **Privacy notice factors:** The five privacy factors (i.e., type, usage, retention, storage, and access) were specified as bullet points. Data type, usage, and access have icons and text, while data retention and storage have only text.
- **Presentation:** We used a combination of icons and short description text to simplify the presentation of the privacy information.
- **Framing:** We used a label format and bullet points to frame the privacy information. We further used bold and different colours to highlight the privacy policy text.
- **Interaction:** We used hovering over the icons as the interaction feature to convey more privacy information to the users.

It is important to note that different types of privacy visualisations can be used for each component based on their characteristics. We do not claim generalization by providing the toolkit and the three examples above, as this toolkit needs to be tested in multiple domains. However, our privacy management visualisation toolkit synthesizes the key privacy elements highlighted in previous research into a single knowledge base. The knowledge base not only captures the most important privacy notice factors but also correlates with how these factors can be visualised to users based on previous research. Figure 12 depicts a Sankey diagram of the articles from which we extracted the privacy visualisation management toolkit elements (i.e., privacy factors described in the literature (Table 2) along with what the literature used to visualise the privacy information (Table 5)). As shown in Figure 5, when the camera collects data, the data goes through complex processing involving storage and retention. Considering the toolkit, which shows privacy factors, how to visualise them, and the goal of visualising them (awareness, control, or both), can help developers create effective privacy notices.

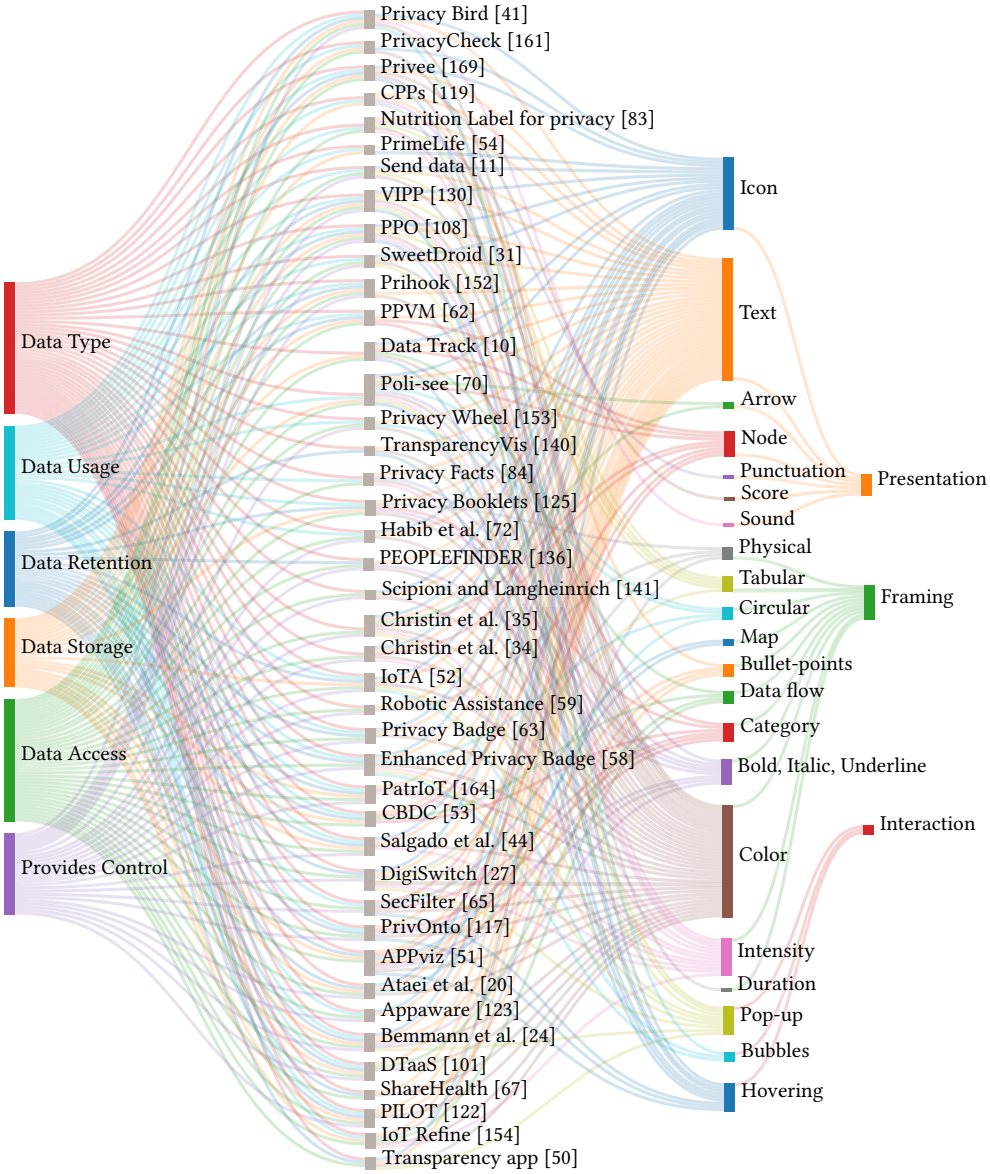

Fig. 12. A Sankey diagram of privacy visualisation management toolkit depicting the privacy factors described in the literature along with what the literature used to visualise the privacy information.

6 DISCUSSION

According to the literature we reviewed (see Table 2), most visualisation solutions were developed for the Web and mobile platforms, with fewer efforts made in the IoT domain. Given the exponential growth of IoT devices and IoT sensors' ability to sweep data without the user's knowledge [28], more IoT privacy visualisation efforts are needed.

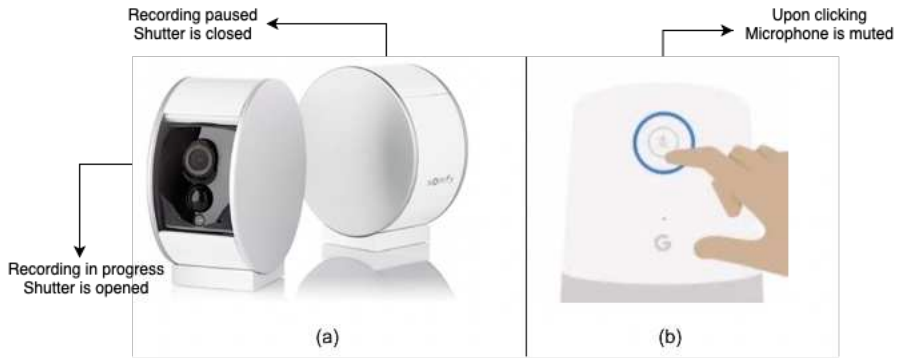

Fig. 13. IoT products that incorporate special features can support preserving an individual's privacy.

Some new solutions are on the market to help users maintain their privacy. Somfy, as shown in Figure 13 (a), created a monitoring camera with a privacy shutter that closes whenever someone enters their private area [147]. They have guaranteed that if the shutter is closed, nothing is recorded or stored in the cloud, [147]. Google has a smart speaker, as shown in Figure 13 (b), with a physical microphone switch that can be turned on and off as desired by the user [66]. It can be challenging to assume that all IoT devices will have a privacy feature because each device is equipped with different sensors [68]. However, it is critical to have a common phenomenon of protecting user privacy and informing users about any related means of data collection, which is the primary goal of the privacy management toolkit proposed in this paper. As available research focuses on developing notification methods that are simple to understand, do not disrupt the user, and increase user awareness [48]. We set the groundwork for future researchers and developers to create effective privacy notices in this paper. Manufacturers of IoT devices should collaborate with application developers to meet the privacy needs of end-users.

Throughout the device development cycle, IoT developers and manufacturers must consider the device's privacy and how it may impact users. This information must be communicated to users in an understandable manner by using, for example, the three-step design shown in Figure 11 (i). Sensors in the connected world have introduced new data collection methods, resulting in multiple privacy issues. Adopting the P3P protocol ontology, as previously described, could also help address some of these issues. For example, one of the essential features of the P3P protocol [79] was giving the user the option to control their data. Although the P3P is a web-based tool, its mechanism can aid in reducing privacy concerns in the IoT domain [61, 91].

7 RESEARCH CHALLENGES AND OPPORTUNITIES

With the introduction of new modes of interaction via IoT devices, people face difficulties comprehending the underlying concept of these interactions [42, 55, 148]. As tabulated in Tables 2 and 5, the notification mechanism is widely used in the digital space to inform users about how websites use their data [83]. Users surfing the web, for example, are usually informed that their data is being collected and used to provide them with the service. Furthermore, most users access web services on purpose, with their knowledge and consent. However, this is not the case in the context of IoT [47]. IoT devices and sensors are widely used, installed in physical spaces, and are small in size, making them ideal for going unnoticed [83]. In this section, we elaborate on the gaps discussed previously and present some of the research challenges and opportunities for future research.

7.1 Legalizing Privacy visualisations

Privacy regulations, such as the General Data Protection Regulation (GDPR) [129] and the California Consumer Privacy Act (CCPA) [30], mandate privacy notices when collecting user data. However, privacy notices are often ignored or abandoned by users [139]. Several studies have found that available privacy notices fall short due to their lengthy and difficult-to-read presentation [138]. Consequently, as shown in Tables 2 and 5, many efforts offer privacy policy visualisations and notification methods to capture users' attention and increase their awareness. Yet, except for the *Nutrition Label for privacy* [83], which Apple has adopted [96], other privacy policy visualisations have little to no adoption [23].

Barth et al. [23] discussed that privacy visualisations will become widespread only with a legal mandate. We speculate that legalizing the adoption of such privacy visualisations can help users understand IoT privacy. By proposing the toolkit, we highlight the common visualisation elements to help developers provide effective privacy notices that can be legalized in the future. Although we cannot force users' attention, the studies in Tables 2 and 5 show that better privacy visualisations can effectively increase users' awareness. Using the toolkit can potentially produce an effective privacy visualisation that could provide users with the resources to understand the privacy implications of their IoT devices.

7.2 Development Language

A significant challenge that arises with the IoT emergence is the diverse nature of its developers [19]. IoT devices in the market are not only developed by known reputable companies that have access to resources but also are developed by small entities that may lack essential resources and/or experience [19]. Consequently, almost all levels of society acquire and use IoT devices [143, 162]. So, to have an IoT device that supports the user's privacy, it is essential to employ a privacy policies development language that is fast and reliable [7]. More importantly, a privacy policy development language that contains the necessary privacy information to serve both the developer and the device user is required.

As described earlier, the P3P protocol gives the user control regarding the use of their data. The inclusion of P3P into the IoT domain as a means of raising individual awareness has been proposed by Langheinrich [91]. Langheinrich proposed a model that uses the P3P machine-readable privacy policies to communicate with nearby IoT sensors, allowing the users to manage their preferences regarding their personal information. Ghazinour et al. [61] have built upon the use of P3P in presenting a model that not only provides the privacy policy to the user but also ensures the enforcement of the use of the privacy policy by both the user and the service provider. Other languages, such as EPAL [17] and PPVM [62] have also incorporated privacy policies that can support the IoT domain. Although with the IoT sensors, there is a considerable amount of sensed data, it is practical to have the employment of the P3P protocol due to the fact that the enforcement of policy is usually task-based.

Various development languages are available for developers, such as [15, 85, 155, 157]. Although these languages are powerful, they rely heavily on web-based tools and are aimed at people with a technical background [110]. Because IoT devices, particularly small and unnoticeable devices, are developed by individuals and small businesses, privacy concerns are frequently overlooked due to their cost and complexity. Moreover, the developers of these devices have limited experience with device privacy updates [74]. Will having a privacy policy development language that is reliable and cost-effective help in incorporating the privacy requirements into the IoT devices? Is it possible that there are templates that must be followed for a device to pass a privacy check? Will the involvement of a third party help in tackling this issue?

7.3 Interaction Patterns and Personalisation

Capturing the interaction pattern between an individual and the IoT device can be used to improve device awareness for a user [69]. This interaction pattern should be reliable and effectively communicate data flow to and from a device [91]. The interaction pattern must also be readily deployable, considering the sensors' size and the device user's experience. Can there be an interaction pattern that conveys to the user an essential device's functionality in a straightforward way, e.g., a privacy label with well-known icons indicating data collection, red blinking light indicating sensitive data collection, or a loud sound indicating an urgently needed interaction? Can the interaction pattern cope with the increase in the number of sensors acquired by a single individual? Can we have a cost-effective model that balances the number of needed notifications with user annoyance?

The availability of such an interaction pattern requires understanding both the user and the device [69]. In the case of IoT, a comprehensive understanding of the users' social context and the IoT sensor functionality is a must [69]. That is because the IoT sensors are shared in nature, i.e., either deployed in a shared space or used by more than one person [87]. There exist multiple designs and frameworks that support understanding individuals' awareness levels, such as [16, 26, 37, 78, 113, 171]. However, most of these frameworks are designed for experienced developers and users, making them difficult to implement in the IoT domain. Furthermore, existing frameworks and designs are difficult to implement in IoT shared spaces.

While privacy policies must inform users about the possibility of data collection and disclosure [30, 129], guidance on which tools to use and how to use them for presenting privacy notices is limited. The privacy management toolkit presented in Section 5.2 is based on a thorough review and comparison of privacy factors and notification methods covered by literature (see Figure 12) targeted at online, mobile, and IoT services. Hence, it represents a comprehensive checklist of privacy notice visualisation aspects and may simplify the privacy awareness check for both developers and IoT device users. The toolkit can function as a catalogue of various types of privacy management visualisation, from which the developer and/or device user can create or select recommended personalised patterns based on their requirements. A valuable research direction is to examine whether such a toolkit can be used as a foundation for developers to consider individuals' privacy when developing an IoT device. Additionally, future research could investigate whether this toolkit can be used as a checklist to verify privacy policies' effectiveness [3], structure privacy policies, or improve their readability [170].

8 CONCLUSION

In this survey, we reviewed a wide range of available literature on various mechanisms for visualizing user privacy. The goal is to provide a study that will help in raising awareness and control for IoT users. We began by reviewing the visualisation solutions for privacy management (awareness and control) available on the web, mobile and IoT. Following the review, we identified five major factors that should be considered when developing any privacy notice and/or policy. These factors include the type of data collected, the purpose of data collection, the location of data storage, the data retention period and the data access. This paper defines and illustrates each of these factors in the context of using IoT devices.

In addition, we reviewed the literature on notification method visualisations. From that, we presented a three-step design (presentation, framing, and interaction) that most existing privacy notification visualisations have adopted. This paper also introduces a privacy management toolkit, which can help developers and future researchers design and develop an effective privacy notice. The survey also revealed a number of gaps and challenges, and proposed opportunities that could serve as future research questions and aid in filling the identified gaps.

REFERENCES

[1] Acquisti, A., Adjerid, I., Balebako, R., Brandimarte, L., Cranor, L. F., Komanduri, S., Leon, P. G., Sadeh, N., Schaub, F., Sleeper, M., et al. Nudges for privacy and security: Understanding and assisting users' choices online. *ACM Computing Surveys (CSUR) 50*, 3 (2017), 1–41.

[2] Ahmadian, A. S., Strüber, D., Riediger, V., and Jürjens, J. Supporting privacy impact assessment by model-based privacy analysis. In *Proceedings of the 33rd Annual ACM Symposium on Applied Computing* (2018), pp. 1467–1474.

[3] Al-Jamal, M., and Abu-Shanab, E. Privacy policy of e-government websites: An itemized checklist proposed and tested. *Management Research and Practice 7*, 3 (2015), 80.

[4] Al Muhander, B., Rana, O., Arachchilage, N., and Perera, C. Demo abstract: Privacycube: a tangible device for improving privacy awareness in iot. In *2022 IEEE/ACM Seventh International Conference on Internet-of-Things Design and Implementation (IoTDI)* (2022), IEEE, pp. 109–110.

[5] Alam, M. R., Reaz, M. B. I., and Ali, M. A. M. A review of smart homes—past, present, and future. *IEEE transactions on systems, man, and cybernetics, part C (applications and reviews) 42*, 6 (2012), 1190–1203.

[6] Alhazmi, A., and Arachchilage, N. A. G. I'm all ears! listening to software developers on putting gdpr principles into software development practice. *Personal and Ubiquitous Computing* (2021), 1–14.

[7] Alhirabi, N., Rana, O., and Perera, C. Security and privacy requirements for the internet of things: A survey. *ACM Transactions on Internet of Things 2*, 1 (2021), 1–37.

[8] Alwarafy, A., Al-Thelaya, K. A., Abdallah, M., Schneider, J., and Hamdi, M. A survey on security and privacy issues in edge computing-assisted internet of things. *IEEE Internet of Things Journal* (2020).

[9] Angelelli, M., Catalano, C., Hill, D., Koshutanski, H., Pascarelli, C., and Rafferty, J. A reference architecture proposal for secure data management in mobile health. In *2022 7th International Conference on Smart and Sustainable Technologies (SpliTech)* (2022), IEEE, pp. 1–6.

[10] Angulo, J., Fischer-Hübner, S., Pulls, T., and Wästlund, E. Usable transparency with the data track: a tool for visualizing data disclosures. In *Proceedings of the 33rd Annual ACM Conference Extended Abstracts on Human Factors in Computing Systems* (2015), pp. 1803–1808.

[11] Angulo, J., Fischer-Hübner, S., Wästlund, E., and Pulls, T. Towards usable privacy policy display and management. *Information Management & Computer Security* (2012).

[12] Apthorpe, N., Reisman, D., and Feamster, N. A smart home is no castle: Privacy vulnerabilities of encrypted iot traffic. *arXiv preprint arXiv:1705.06805* (2017).

[13] Arbabi, M. S., Lal, C., Veeraragavan, N. R., Marijan, D., Nygård, J. F., and Vitenberg, R. A survey on blockchain for healthcare: Challenges, benefits, and future directions. *IEEE Communications Surveys & Tutorials* (2022).

[14] Ardito, C., Desolda, G., Lanzilotti, R., Malizia, A., Matera, M., Buono, P., and Piccinno, A. User-defined semantics for the design of iot systems enabling smart interactive experiences. *Personal and Ubiquitous Computing 24*, 6 (2020), 781–796.

[15] Arnold, K., Gosling, J., Holmes, D., and Holmes, D. *The Java programming language*, vol. 2. Addison-wesley Reading, 2000.

[16] Arora, J., Mathur, K., Goel, M., Kumar, P., Mishra, A., and Parnami, A. Design and evaluation of dio construction toolkit for co-making shared constructions. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies 3*, 4 (2019), 1–25.

[17] Ashley, P., Hada, S., Karjoth, G., Powers, C., and Schunter, M. Enterprise privacy authorization language (epal). *IBM Research 30* (2003), 31.

[18] Asquith, N. Understanding the role of verbal and textual hostility in hate crime regulation, 2013.

[19] Assal, H., and Chiasson, S. 'think secure from the beginning' a survey with software developers. In *Proceedings of the 2019 CHI conference on human factors in computing systems* (2019), pp. 1–13.

[20] Ataei, M., Degbelo, A., and Kray, C. Privacy theory in practice: designing a user interface for managing location privacy on mobile devices. *Journal of Location Based Services 12*, 3-4 (2018), 141–178.

[21] Atlam, H. F., and Wills, G. B. Iot security, privacy, safety and ethics. In *Digital Twin Technologies and Smart Cities*. Springer, 2020, pp. 123–149.

[22] Bai, J., Deak, J. G., Iv, H., and Shen, W. Magnetoresistive gear tooth sensor, Aug. 28 2018. US Patent 10,060,941.

[23] Barth, S., Ionita, D., and Hartel, P. Understanding online privacy—a systematic review of privacy visualizations and privacy by design guidelines. *ACM Computing Surveys (CSUR) 55*, 3 (2022), 1–37.

[24] Bemmann, F., Windl, M., Erbe, J., Mayer, S., and Hussmann, H. The influence of transparency and control on the willingness of data sharing in adaptive mobile apps. *Proceedings of the ACM on Human-Computer Interaction 6*, MHCI (2022), 1–26.

[25] Böhmer, M., Lander, C., Gehring, S., Brumby, D. P., and Krüger, A. Interrupted by a phone call: exploring designs for lowering the impact of call notifications for smartphone users. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2014), pp. 3045–3054.

[26] Borchers, J. O. A pattern approach to interaction design. In *Cognition, Communication and Interaction*. Springer, 2008, pp. 114–131.

[27] Caine, K. E., Zimmerman, C. Y., Schall-Zimmerman, Z., Hazlewood, W. R., Jean Camp, L., Connelly, K. H., Huber, L. L., and Shankar, K. Digiswitch: A device to allow older adults to monitor and direct the collection and transmission of health information collected at home. *Journal of medical systems 35*, 5 (2011), 1181–1195.

[28] Calo, R. Against notice skepticism in privacy (and elsewhere). *Notre Dame L. Rev. 87* (2011), 1027.

[29] Cao, H., and Wachowicz, M. An edge-fog-cloud architecture of streaming analytics for internet of things applications. *Sensors 19*, 16 (2019), 3594.

[30] CCPA, D. U. California consumer privacy act (ccpa) website policy. *Policy* (2020).

[31] Chen, X., Huang, H., Zhu, S., Li, Q., and Guan, Q. Sweetdroid: Toward a context-sensitive privacy policy enforcement framework for android os. In *Proceedings of the 2017 on Workshop on Privacy in the Electronic Society* (2017), pp. 75–86.

[32] Chernyshov, G., Chen, J., Lai, Y., Noriyasu, V., and Kunze, K. Ambient rhythm: Melodic sonification of status information for iot-enabled devices. In *Proceedings of the 6th International Conference on the Internet of Things* (2016), pp. 1–6.

[33] Chinnasamy, P., Deepalakshmi, P., Dutta, A. K., You, J., and Joshi, G. P. Ciphertext-policy attribute-based encryption for cloud storage: Toward data privacy and authentication in ai-enabled iot system. *Mathematics 10*, 1 (2021), 68.

[34] Christin, D., Michalak, M., and Hollick, M. Raising user awareness about privacy threats in participatory sensing applications through graphical warnings. In *Proceedings of International Conference on Advances in Mobile Computing & Multimedia* (2013), pp. 445–454.

[35] Christin, D., Reinhardt, A., Hollick, M., and Trumpold, K. Exploring user preferences for privacy interfaces in mobile sensing applications. In *Proceedings of the 11th International Conference on Mobile and Ubiquitous Multimedia* (2012), pp. 1–10.

[36] Chu, G., Apthorpe, N., and Feamster, N. Security and privacy analyses of internet of things children's toys. *IEEE Internet of Things Journal 6*, 1 (2018), 978–985.

[37] Chung, E. S., Hong, J. I., Lin, J., Prabaker, M. K., Landay, J. A., and Liu, A. L. Development and evaluation of emerging design patterns for ubiquitous computing. In *Proceedings of the 5th conference on Designing interactive systems: processes, practices, methods, and techniques* (2004), pp. 233–242.

[38] Cila, N., Smit, I., Giaccardi, E., and Kröse, B. Products as agents: metaphors for designing the products of the iot age. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems* (2017), pp. 448–459.

[39] Consortium, W. W. W., et al. P3p 1.0: A new standard in online privacy.

[40] Corno, F., De Russis, L., and Montanaro, T. A context and user aware smart notification system. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (2015), IEEE, pp. 645–651.

[41] Cranor, L. F., Guduru, P., and Arjula, M. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI) 13*, 2 (2006), 135–178.

[42] Curran, D. Are your phone camera and microphone spying on you. *The Guardian. Available at: https://www. theguardian. com/commentisfree/2018/apr/06/phone-camera-microphone-spying [Accessed 14 Apr 2019]* (2018).

[43] Dang, L. M., Min, K., Wang, H., Piran, M. J., Lee, C. H., and Moon, H. Sensor-based and vision-based human activity recognition: A comprehensive survey. *Pattern Recognition 108* (2020), 107561.

[44] de Lima Salgado, A., Dias, F. S., Mattos, J. P. R., de Mattos Fortes, R. P., and Hung, P. C. Smart toys and children's privacy: usable privacy policy insights from a card sorting experiment. In *Proceedings of the 37th ACM International Conference on the Design of Communication* (2019), pp. 1–8.

[45] Dermadoctor. Dermatologist formulated skin care and skin health advice from Dr. Audrey Kunin.

[46] Edwards, L. Switching off the surveillance society? legal regulation of cctv in the uk. Asser Press, 2005.

[47] Edwards, L. Privacy, security and data protection in smart cities: A critical eu law perspective. *Eur. Data Prot. L. Rev. 2* (2016), 28.

[48] Emami-Naeini, P., Dixon, H., Agarwal, Y., and Cranor, L. F. Exploring how privacy and security factor into iot device purchase behavior. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems* (2019), pp. 1–12.

[49] Emsenhuber, B., and Ferscha, A. Olfactory interaction zones. In *Conf. on Pervasive Computing* (2009).

[50] Escher, S., Etzrodt, K., Weller, B., Köpsell, S., and Strufe, T. Transparency for bystanders in iot regarding audiovisual recordings. In *2022 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)* (2022), IEEE, pp. 649–654.

[51] Eze, C., Nurse, J. R., and Happa, J. Using visualizations to enhance users' understanding of app activities on android devices. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA) 7*, 1 (2016).

[52] Feng, Y., Yao, Y., and Sadeh, N. A design space for privacy choices: Towards meaningful privacy control in the

internet of things. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–16.
[53] Fernández, M., Jaimunk, J., and Thuraisingham, B. Graph-based data-collection policies for the internet of things. In *Proceedings of the 4th Annual Industrial Control System Security Workshop* (2018), pp. 9–16.
[54] Fischer Hübner, S., and Zwingelberg, H. Ui prototypes: Policy administration and presentation-version 2, 2010.
[55] Fruchter, N., and Liccardi, I. Consumer attitudes towards privacy and security in home assistants. In *Extended Abstracts of the 2018 CHI Conference on Human Factors in Computing Systems* (2018), pp. 1–6.
[56] Garcia, D., Toledo, M. B. F., Capretz, M. A., Allison, D. S., Blair, G. S., Grace, P., and Flores, C. Towards a base ontology for privacy protection in service-oriented architecture. In *2009 IEEE International Conference on Service-Oriented Computing and Applications (SOCA)* (2009), IEEE, pp. 1–8.
[57] Gartner. he internet of things (iot)* units installed base by category from 2014 to 2020 (in billions). *Statista Chart* (Feb. 2017).
[58] Gehring, S., and Gisch, M. The privacy badge revisited-enhancement of a privacy-awareness user interface for small devices. In *Proceedings of the Workshop on Security and Privacy Issues in Mobile Phone Use* (2008), Citeseer, p. 8.
[59] Georgievski, I., Jeyakumar, I. H. J., and Kale, S. Designing a system based on robotic assistance for privacy awareness in smart environments. In *2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (2021), IEEE, pp. 0427–0432.
[60] Ghazal, T. M., Hasan, M. K., Alshurideh, M. T., Alzoubi, H. M., Ahmad, M., Akbar, S. S., Al Kurdi, B., and Akour, I. A. Iot for smart cities: Machine learning approaches in smart healthcare—a review. *Future Internet 13*, 8 (2021), 218.
[61] Ghazinour, K., Majedi, M., and Barker, K. A lattice-based privacy aware access control model. In *2009 International Conference on Computational Science and Engineering* (2009), vol. 3, IEEE, pp. 154–159.
[62] Ghazinour, K., Majedi, M., and Barker, K. A model for privacy policy visualization. In *2009 33rd Annual IEEE International Computer Software and Applications Conference* (2009), vol. 2, IEEE, pp. 335–340.
[63] Gisch, M., De Luca, A., and Blanchebarbe, M. The privacy badge: a privacy-awareness user interface for small devices. In *Proceedings of the 4th international conference on mobile technology, applications, and systems and the 1st international symposium on Computer human interaction in mobile technology* (2007), pp. 583–586.
[64] Gomulkiewicz, R. W., and Williamson, M. L. A brief defense of mass market software license agreements. *Rutgers Computer & Tech. LJ 22* (1996), 335.
[65] Gonzalez-Compean, J., Telles, O., Lopez-Arevalo, I., Morales-Sandoval, M., Sosa-Sosa, V. J., and Carretero, J. A policy-based containerized filter for secure information sharing in organizational environments. *Future Generation Computer Systems 95* (2019), 430–444.
[66] Google. Privacy Features of Google Home Mini – Google Store.
[67] Greene, E., Proctor, P., and Kotz, D. Secure sharing of mhealth data streams through cryptographically-enforced access control. *Smart Health 12* (2019), 49–65.
[68] Gulati, K., Boddu, R. S. K., Kapila, D., Bangare, S. L., Chandnani, N., and Saravanan, G. A review paper on wireless sensor network techniques in internet of things (iot). *Materials Today: Proceedings 51* (2022), 161–165.
[69] Guo, B., Zhang, D., Yu, Z., Liang, Y., Wang, Z., and Zhou, X. From the internet of things to embedded intelligence. *World Wide Web 16*, 4 (2013), 399–420.
[70] Guo, W., Rodolitz, J., and Birrell, E. Poli-see: An interactive tool for visualizing privacy policies. In *Proceedings of the 19th Workshop on Privacy in the Electronic Society* (2020), pp. 57–71.
[71] Gupta, R., Gupta, I., Singh, A. K., Saxena, D., and Lee, C.-N. An iot-centric data protection method for preserving security and privacy in cloud. *IEEE Systems Journal* (2022).
[72] Habib, H., Zou, Y., Yao, Y., Acquisti, A., Cranor, L., Reidenberg, J., Sadeh, N., and Schaub, F. Toggles, dollar signs, and triangles: How to (in) effectively convey privacy choices with icons and link texts. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems* (2021), pp. 1–25.
[73] Haslgrübler, M., Fritz, P., Gollan, B., and Ferscha, A. Getting through: modality selection in a multi-sensor-actuator industrial iot environment. In *Proceedings of the Seventh International Conference on the Internet of Things* (2017), pp. 1–8.
[74] Hong, J. The privacy landscape of pervasive computing. *IEEE Pervasive Computing 16*, 3 (2017), 40–48.
[75] Houben, S., Golsteijn, C., Gallacher, S., Johnson, R., Bakker, S., Marquardt, N., Capra, L., and Rogers, Y. Physikit: Data engagement through physical ambient visualizations in the home. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (2016), pp. 1608–1619.
[76] HowStuffWorks. How Amazon Echo Works | HowStuffWorks.
[77] Huang, H., and Ng, K. H. Designing for cultural learning and reflection using iot serious game approach. *Personal and Ubiquitous Computing* (2020), 1–16.
[78] Iachello, G., and Abowd, G. D. From privacy methods to a privacy toolbox: Evaluation shows that heuristics are complementary. *ACM Transactions on Computer-Human Interaction (TOCHI) 15*, 2 (2008), 1–30.

[79] Jamtgaard, L. *The P3P Implementation Guide*. 2003.
[80] Jeong, J. J., Oliver, G., Kang, E., Creese, S., and Thomas, P. The current state of research on people, culture and cybersecurity, 2021.
[81] Kacsmar, B., Tilbury, K., Mazmudar, M., and Kerschbaum, F. Caring about sharing: User perceptions of multiparty data sharing. In *31st USENIX Security Symposium (USENIX Security 22)* (2022), pp. 899–916.
[82] Kaushik, K., and Dahiya, S. Security and privacy in iot based e-business and retail. In *2018 International Conference on System Modeling & Advancement in Research Trends (SMART)* (2018), IEEE, pp. 78–81.
[83] Kelley, P. G., Bresee, J., Cranor, L. F., and Reeder, R. W. A" nutrition label" for privacy. In *Proceedings of the 5th Symposium on Usable Privacy and Security* (2009), pp. 1–12.
[84] Kelley, P. G., Cranor, L. F., and Sadeh, N. Privacy as part of the app decision-making process. In *Proceedings of the SIGCHI conference on human factors in computing systems* (2013), pp. 3393–3402.
[85] Kernighan, B. W., Ritchie, D. M., et al. *The C programming language*, vol. 2. prentice-Hall Englewood Cliffs, NJ, 1988.
[86] Kilic, D., Crabtree, A., McGarry, G., and Goulden, M. The cardboard box study: Understanding collaborative data management in the connected home. pp. 1–32.
[87] Kilic, D., Crabtree, A., McGarry, G., and Goulden, M. The cardboard box study: understanding collaborative data management in the connected home. *Personal and Ubiquitous Computing 26*, 1 (2022), 155–176.
[88] Kowalski, R., Loehmann, S., and Hausen, D. Cubble: A multi-device hybrid approach supporting communication in long-distance relationships. In *Proceedings of the 7th International Conference on Tangible, Embedded and Embodied Interaction* (2013), pp. 201–204.
[89] Kubitza, T., Voit, A., Weber, D., and Schmidt, A. An iot infrastructure for ubiquitous notifications in intelligent living environments. In *Proceedings of the 2016 ACM international joint conference on pervasive and ubiquitous computing: Adjunct* (2016), pp. 1536–1541.
[90] Kumari, A., Tanwar, S., Tyagi, S., Kumar, N., Maasberg, M., and Choo, K.-K. R. Multimedia big data computing and internet of things applications: A taxonomy and process model. *Journal of Network and Computer Applications 124* (2018), 169–195.
[91] Langheinrich, M. A privacy awareness system for ubiquitous computing environments. In *international conference on Ubiquitous Computing* (2002), Springer, pp. 237–245.
[92] Lee, H., and Kobsa, A. Privacy preference modeling and prediction in a simulated campuswide iot environment. In *2017 IEEE International Conference on Pervasive Computing and Communications (PerCom)* (2017), IEEE, pp. 276–285.
[93] Lee, H., and Kobsa, A. Confident privacy decision-making in iot environments. *ACM Transactions on Computer-Human Interaction (TOCHI) 27*, 1 (2019), 1–39.
[94] Lee, H., and Lee, U. Toward dynamic consent for privacy-aware pervasive health and well-being: A scoping review and research directions. *IEEE Pervasive Computing* (2022).
[95] Leon, P. G., Ur, B., Wang, Y., Sleeper, M., Balebako, R., Shay, R., Bauer, L., Christodorescu, M., and Cranor, L. F. What matters to users? factors that affect users' willingness to share information with online advertisers. In *Proceedings of the ninth symposium on usable privacy and security* (2013), pp. 1–12.
[96] Li, Y., Chen, D., Li, T., Agarwal, Y., Cranor, L. F., and Hong, J. I. Understanding ios privacy nutrition labels: An exploratory large-scale analysis of app store data. In *CHI Conference on Human Factors in Computing Systems Extended Abstracts* (2022), pp. 1–7.
[97] Lin, J., Yu, W., Zhang, N., Yang, X., Zhang, H., and Zhao, W. A survey on internet of things: Architecture, enabling technologies, security and privacy, and applications. *IEEE Internet of Things Journal 4*, 5 (2017), 1125–1142.
[98] Lipford, H. R., Tabassum, M., Bahirat, P., Yao, Y., and Knijnenburg, B. P. Privacy and the internet of things. In *Modern Socio-Technical Perspectives on Privacy*. Springer, Cham, 2022, pp. 233–264.
[99] Liu, L., Zhu, H., Chen, S., and Huang, Z. Privacy regulation aware service selection for multi-provision cloud service composition. *Future Generation Computer Systems 126* (2022), 263–278.
[100] Lodge, T., and Crabtree, A. Privacy engineering for domestic iot: Enabling due diligence. *Sensors 19*, 20 (2019), 4380.
[101] Lomotey, R. K., Kumi, S., and Deters, R. Data trusts as a service: Providing a platform for multi-party data sharing. *International Journal of Information Management Data Insights 2*, 1 (2022), 100075.
[102] Luria, M., Hoffman, G., and Zuckerman, O. Comparing social robot, screen and voice interfaces for smart-home control. In *Proceedings of the 2017 CHI conference on human factors in computing systems* (2017), pp. 580–628.
[103] Marannan, A., Nagarajan, M., and Nayek, P. Study on software agreement (eula).
[104] Matscheko, M., Ferscha, A., Riener, A., and Lehner, M. Tactor placement in wrist worn wearables. In *International Symposium on Wearable Computers (ISWC) 2010* (2010), IEEE, pp. 1–8.
[105] McKinnon, D., and Turp, C. Are library vendors doing enough to protect users? a content analysis of major ils privacy policies. *The Journal of Academic Librarianship 48*, 2 (2022), 102505.

[106] Mehta, V., Bandara, A. K., Price, B. A., and Nuseibeh, B. Privacy itch and scratch: on body privacy warnings and controls. In *Proceedings of the 2016 CHI Conference Extended Abstracts on Human Factors in Computing Systems* (2016), pp. 2417–2424.

[107] Menard, P., and Bott, G. J. Analyzing iot users' mobile device privacy concerns: Extracting privacy permissions using a disclosure experiment. *Computers & Security 95* (2020), 101856.

[108] Mohammadi, N. G., Pampus, J., and Heisel, M. Pattern-based incorporation of privacy preferences into privacy policies: negotiating the conflicting needs of service providers and end-users. In *Proceedings of the 24th European Conference on Pattern Languages of Programs* (2019), pp. 1–12.

[109] Muñoz-Cristóbal, J. A., Rodríguez-Triana, M. J., Gallego-Lema, V., Arribas-Cubero, H. F., Asensio-Pérez, J. I., and Martínez-Monés, A. Monitoring for awareness and reflection in ubiquitous learning environments. *International Journal of Human–Computer Interaction 34*, 2 (2018), 146–165.

[110] Naeini, P. E., Bhagavatula, S., Habib, H., Degeling, M., Bauer, L., Cranor, L. F., and Sadeh, N. Privacy expectations and preferences in an iot world. In *Thirteenth Symposium on Usable Privacy and Security ({SOUPS} 2017)* (2017), pp. 399–412.

[111] Neisse, R., Baldini, G., Steri, G., Miyake, Y., Kiyomoto, S., and Biswas, A. R. An agent-based framework for informed consent in the internet of things. In *2015 IEEE 2nd World Forum on Internet of Things (WF-IoT)* (2015), IEEE, pp. 789–794.

[112] NEWS, C. Ring security system program with law enforcement raises privacy concerns. *CBS NEWS* (Aug. 2019).

[113] Niemantsverdriet, K., Essen, H. V., Pakanen, M., and Eggen, B. Designing for awareness in interactions with shared systems: the dass framework. *ACM Transactions on Computer-Human Interaction (TOCHI) 26*, 6 (2019), 1–41.

[114] Nouwens, M., Liccardi, I., Veale, M., Karger, D., and Kagal, L. Dark patterns after the gdpr: Scraping consent pop-ups and demonstrating their influence. In *Proceedings of the 2020 CHI conference on human factors in computing systems* (2020), pp. 1–13.

[115] Nower, N. Privacy in iot: Expectations, causes of concerns, and reasons for concern mitigation. *International Journal of Computer Applications 975* (2019), 8887.

[116] Olalere, I. O., Dewa, M., and Nleya, B. Remote condition monitoring of elevator's vibration and acoustics parameters for optimised maintenance using iot technology. In *2018 IEEE Canadian Conference on Electrical & Computer Engineering (CCECE)* (2018), IEEE, pp. 1–4.

[117] Oltramari, A., Piraviperumal, D., Schaub, F., Wilson, S., Cherivirala, S., Norton, T. B., Russell, N. C., Story, P., Reidenberg, J., and Sadeh, N. Privonto: A semantic framework for the analysis of privacy policies. *Semantic Web 9*, 2 (2018), 185–203.

[118] Onu, E., Kwakye, M. M., and Barker, K. Contextual privacy policy modeling in iot. In *2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (2020), IEEE, pp. 94–102.

[119] Ortloff, A.-M., Windl, M., Schwind, V., and Henze, N. Implementation and in situ assessment of contextual privacy policies. In *Proceedings of the 2020 ACM Designing Interactive Systems Conference* (2020), pp. 1765–1778.

[120] Pal, K., et al. Internet of things and blockchain technology in apparel manufacturing supply chain data management. *Procedia Computer Science 170* (2020), 450–457.

[121] Pardo, A., and Siemens, G. Ethical and privacy principles for learning analytics. *British journal of educational technology 45*, 3 (2014), 438–450.

[122] Pardo, R., and Métayer, D. L. Analysis of privacy policies to enhance informed consent. In *IFIP Annual Conference on Data and Applications Security and Privacy* (2019), Springer, pp. 177–198.

[123] Paspatis, I., Tsohou, A., and Kokolakis, S. Appaware: a policy visualization model for mobile applications. *Information & Computer Security* (2020).

[124] Paul, A., and Jeyaraj, R. Internet of things: A primer. *Human Behavior and Emerging Technologies 1*, 1 (2019), 37–47.

[125] Pierce, J., Fox, S., Merrill, N., Wong, R., and DiSalvo, C. An interface without a user: An exploratory design study of online privacy policies and digital legalese. In *Proceedings of the 2018 Designing Interactive Systems Conference* (2018), pp. 1345–1358.

[126] Pousman, Z., and Stasko, J. A taxonomy of ambient information systems: four patterns of design. In *Proceedings of the working conference on Advanced visual interfaces* (2006), pp. 67–74.

[127] Qiu, J., Tian, Z., Du, C., Zuo, Q., Su, S., and Fang, B. A survey on access control in the age of internet of things. *IEEE Internet of Things Journal 7*, 6 (2020), 4682–4696.

[128] Reagle, J., and Cranor, L. F. The platform for privacy preferences. *Communications of the ACM 42*, 2 (1999), 48–55.

[129] Regulation, P. Regulation (eu) 2016/679 of the european parliament and of the council. *Regulation (eu) 679* (2016), 2016.

[130] Reinhardt, D., Borchard, J., and Hurtienne, J. Visual interactive privacy policy: The better choice? In *Proceedings*

of the 2021 CHI Conference on Human Factors in Computing Systems (2021), pp. 1–12.

[131] Reinsel, D., Gantz, J., and Rydning, J. The digitization of the world from edge to core). *IDC White Paper by Seagate* (Nov. 2018).

[132] Ring. Video Doorbell – Ring.

[133] Rizi, M. H. P., and Seno, S. A. H. A systematic review of technologies and solutions to improve security and privacy protection of citizens in the smart city. *Internet of Things* (2022), 100584.

[134] Rodić, L. D., and Granić, A. Tangible interfaces in early years' education: a systematic review. *Personal and Ubiquitous Computing* (2021), 1–39.

[135] Rozendaal, M. C., Boon, B., and Kaptelinin, V. Objects with intent: Designing everyday things as collaborative partners. *ACM Transactions on Computer-Human Interaction (TOCHI) 26*, 4 (2019), 1–33.

[136] Sadeh, N., Hong, J., Cranor, L., Fette, I., Kelley, P., Prabaker, M., and Rao, J. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and ubiquitous computing 13*, 6 (2009), 401–412.

[137] Sahu, K. S., Oetomo, A., and Morita, P. P. Enabling remote patient monitoring through the use of smart thermostat data in canada: exploratory study. *JMIR mHealth and uHealth 8*, 11 (2020), e21016.

[138] Schaub, F., Balebako, R., and Cranor, L. F. Designing effective privacy notices and controls. *IEEE Internet Computing* (2017).

[139] Schaub, F., Balebako, R., Durity, A. L., and Cranor, L. F. A design space for effective privacy notices. In *Eleventh Symposium On Usable Privacy and Security ({SOUPS} 2015)* (2015), pp. 1–17.

[140] Schufrin, M., Reynolds, S. L., Kuijper, A., and Kohlhammer, J. A visualization interface to improve the transparency of collected personal data on the internet. *IEEE Transactions on Visualization and Computer Graphics 27*, 2 (2020), 1840–1849.

[141] Scipioni, M. P., and Langheinrich, M. To share or not to share? an activity-centered approach for designing usable location sharing tools. In *Workshop on Usable Privacy & Security for Mobile Devices (U-PriSM)* (2012).

[142] Seedstudio. Sensors - Seeed Studio Electronics.

[143] Sen, A., and Ahmed, A. A comprehensive privacy and security framework for dynamic protection (cpsf). *International Journal of Information Technology* (2022), 1–9.

[144] Seymour, W., Kraemer, M. J., Binns, R., and Van Kleek, M. Informing the design of privacy-empowering tools for the connected home. In *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems* (2020), pp. 1–14.

[145] Sharma, T., Dyer, H. A., and Bashir, M. Enabling user-centered privacy controls for mobile applications: Covid-19 perspective. *ACM Transactions on Internet Technology (TOIT) 21*, 1 (2021), 1–24.

[146] Sherrick, C. vibrotactile pattern perception: Some findings and. *The psychology of touch* (1991), 189–218.

[147] Somfy. somfy 2401507 Indoor Camera, Full HD Security Camera for Home Security Systems, Smart Device with Integrated App and Simple Installation: Amazon.co.uk: DIY & Tools.

[148] Steinberg, J. These devices may be spying on you (even in your own home). *Forbes, viewed 3* (2014).

[149] Sun, Y., Song, H., Jara, A. J., and Bie, R. Internet of things and big data analytics for smart and connected communities. *IEEE access 4* (2016), 766–773.

[150] Susnjara, B. Fighting crime or invading privacy? police deals with ring video doorbell have advocates and critics. *Daily Herald Media Group* (Feb. 2020).

[151] Thonti, V. Different types of sensors and their working electronics.

[152] Tian, C., Wang, Y., Liu, P., Wang, Y., Dai, R., Zhou, A., and Xu, Z. Prihook: Differentiated context-aware hook placement for different owners' smartphones. In *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)* (2020), IEEE, pp. 615–622.

[153] Van den Berg, B., and Van der Hof, S. What happens to my data? a novel approach to informing users of data processing practices. *First Monday 17*, 7 (2012).

[154] Van Kleek, M., Seymour, W., Binns, R., Zhao, J., Karandikar, D., and Shadbolt, N. Iot refine: Making smart home devices accountable for their data harvesting practices.

[155] Van Rossum, G., et al. Python programming language. In *USENIX annual technical conference* (2007), vol. 41, p. 36.

[156] Vergara-Laurens, I. J., Jaimes, L. G., and Labrador, M. A. Privacy-preserving mechanisms for crowdsensing: Survey and research challenges. *IEEE Internet of Things Journal 4*, 4 (2016), 855–869.

[157] Wilde, M., Hategan, M., Wozniak, J. M., Clifford, B., Katz, D. S., and Foster, I. Swift: A language for distributed parallel scripting. *Parallel Computing 37*, 9 (2011), 633–652.

[158] Wolpert, D. M., Diedrichsen, J., and Flanagan, J. R. Principles of sensorimotor learning. *Nature Reviews Neuroscience 12*, 12 (2011), 739–751.

[159] Wu, L., Du, X., Guizani, M., and Mohamed, A. Access control schemes for implantable medical devices: A survey. *IEEE Internet of Things Journal 4*, 5 (2017), 1272–1283.

[160] Yang, Y., Wu, L., Yin, G., Li, L., and Zhao, H. A survey on security and privacy issues in internet-of-things. *IEEE Internet of Things Journal 4*, 5 (2017), 1250–1258.

[161] Zaeem, R. N., German, R. L., and Barber, K. S. Privacycheck: Automatic summarization of privacy policies using data mining. *ACM Transactions on Internet Technology (TOIT) 18*, 4 (2018), 1–18.

[162] Zainuddin, N., Daud, M., Ahmad, S., Maslizan, M., and Abdullah, S. A. L. A study on privacy issues in internet of things (iot). In *2021 IEEE 5th International Conference on Cryptography, Security and Privacy (CSP)* (2021), IEEE, pp. 96–100.

[163] Zaslavsky, A., Perera, C., and Georgakopoulos, D. Sensing as a service and big data. *arXiv preprint arXiv:1301.0159* (2013).

[164] Zavalyshyn, I., Santos, N., Sadre, R., and Legay, A. My house, my rules: A private-by-design smart home platform. In *MobiQuitous 2020-17th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services* (2020), pp. 273–282.

[165] Zheng, S., Apthorpe, N., Chetty, M., and Feamster, N. User perceptions of smart home iot privacy. *Proceedings of the ACM on Human-Computer Interaction 2*, CSCW (2018), 1–20.

[166] Zheng, X., and Cai, Z. Privacy-preserved data sharing towards multiple parties in industrial iots. *IEEE Journal on Selected Areas in Communications 38*, 5 (2020), 968–979.

[167] Zhou, W., Jia, Y., Peng, A., Zhang, Y., and Liu, P. The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved. *IEEE Internet of Things Journal 6*, 2 (2018), 1606–1616.

[168] Ziegeldorf, J. H., Morchon, O. G., and Wehrle, K. Privacy in the internet of things: threats and challenges. *Security and Communication Networks 7*, 12 (2014), 2728–2742.

[169] Zimmeck, S., and Bellovin, S. M. Privee: An architecture for automatically analyzing web privacy policies. In *23rd USENIX Security Symposium (USENIX Security 14)* (2014), pp. 1–16.

[170] Zimmeck, S., Goldstein, R., and Baraka, D. Privacyflash pro: Automating privacy policy generation for mobile apps. In *NDSS* (2021).

[171] Zimmerman, J. Designing for the self: making products that help people become the person they desire to be. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems* (2009), pp. 395–404.