Designing Privacy-Aware IoT for Unregulated Domains

NADA ALHIRABI, Cardiff University, UK
STEPHANIE BEAUMONT, My Data Fix Ltd, UK
OMER RANA, Cardiff University, UK
CHARITH PERERA, Cardiff University, UK

Internet of things (IoT) applications (apps) are challenging to design because of their heterogeneous deployment systems. In the context of privacy and IoT, there is sensitive data is being collected, with some being collected for highly regulated domains such as health, and others being collected in less regulated domains. IoT apps may collect and analyse personal data, often classified as sensitive, which is protected by data privacy laws. Privacy-by-design (PbD) schemes already exist in various forms, which enable developers to consider data privacy during application design. Developers, however, are not widely adopting these approaches due to difficulties in understanding and interpreting them. In this context, there are currently a limited number of tools available to developers. We believe that a successful privacy design tool should be able to (i) assist developers in designing for privacy even in less regulated domains, as well as (ii) help them learn about privacy as they use the tool. In this paper, we present the findings of two controlled lab studies with 42 developers and discuss how such a PbD tool can help novice IoT developers comply with privacy laws (such as GDPR) and follow privacy guidelines (such as privacy patterns). Based on our findings, such tools might raise awareness of data privacy requirements in design. This increases the likelihood that subsequent designs will be more aware of data privacy requirements. Furthermore, the study illustrates the educational potential of such a tool for educating university novice developers about privacy.

CCS Concepts: • **Security and privacy** → *Privacy protections*; *Domain-specific security and privacy architectures*; • **Software and its engineering** → **System modeling languages**; **Visual languages**; **Domain specific languages**; • **Human-centered computing** → Ubiquitous and mobile computing design and evaluation methods; **Visualization toolkits**.

Additional Key Words and Phrases: Internet of Things, Privacy, Privacy Laws, Tools, Software Design, Software Developers, Data Protection, Unregulated Domains

1 INTRODUCTION

The Internet of Things (IoT) applications generate and process a large amount of data that is transmitted between devices. Due to the heterogeneous nature of IoT systems, their applications are particularly vulnerable to attack. As a result, the associated risks of IoT devices keep evolving with the expansion of their connectivity and availability [31]. With the rapid increase in the size and frequency of this data, an efficient architecture is necessary to handle it [38]. Techno-regulatory approaches have been advocated since the late 1990s to minimize and eliminate privacy risks in data processing systems. Generally, these approaches – commonly referred to as '*privacy-enhancing technologies*' (PETs) – are discussed in conjunction with privacy-by-design (PbD) principles, which are incorporated into legislation for the first time in General Data Protection Regulation (GDPR) under the concept of data protection by design and default (DPbD). The PbD/DPbD concept seeks to ensure that privacy-related requirements are considered when designing and developing data processing systems [12].

Cavoukian [13] recognised the importance of incorporating PbD into the design of information technologies and systems. Therefore, Cavoukian identified seven privacy design principles that can

Authors' addresses: Nada Alhirabi, Cardiff University, School of Computer Science and Informatics, Cardiff, CF24 3AA, UK, alhirabin@cardiff.ac.uk; Stephanie Beaumont, My Data Fix Ltd, Wenlock Road, London, N1 7GU, UK, stephaniebeaumont@mydatafix.com; Omer Rana, Cardiff University, School of Computer Science and Informatics, Cardiff, CF24 3AA, UK, ranaof@cardiff.ac.uk; Charith Perera, Cardiff University, School of Computer Science and Informatics, Cardiff, CF24 3AA, UK, pererac@cardiff.ac.uk.

be applied to PbD. This framework was developed as a means to improve the quality of engineers' designs by increasing their awareness of privacy issues while developing their designs. Since then, efforts have been made to reduce the risks associated with the processing of personal information. Several approaches have been used, including PETs as well as privacy process patterns [18]. Despite the efforts being made in the PbD field, most people are unaware of the potential privacy issues that may arise in an online context. Users, such as developers, often find it difficult to understand privacy policies and their implications [16, 28, 34]. Further, developers rarely discuss privacy concerns with regards to the design or implementation of particular apps [42]. Therefore, there is a need for a privacy-aware tool to increase developers' awareness about privacy requirements [3, 51, 53].

We believe that having a PbD tool can offer intuitive and user-friendly interfaces to assist and educate software developers on how to learn and include privacy in their system design especially in less regulated domains. In our previous research [2, 4], we have captured privacy design requirements to support PbD practices for developers in well-regulated domains (i.e. health). In this work, we worked iteratively with privacy professionals to uncover challenges in less-regulated domains. Moreover, we co-designed with novice developers to identify any potential enhancements to implement for PbD educational tool.

This paper makes the following research contributions:

- Assisting developers in uncovering privacy risks in less regulated domains. Less regulated domains pose more challenges, and we conducted several iterative group studies with a privacy lawyer and privacy professionals to identify these challenges. Our findings allowed us to identify common pitfalls in incorporating privacy when designing IoT applications such as managing advertisements, cookies, and third-party payments.
- Promoting privacy awareness during IoT application design. We conducted two lab studies demonstrating the effectiveness of using a PbD tool. Our findings indicate that the use of the tool leads to a better understanding of personal data handling, which facilitates the development of more privacy-aware IoT solutions.
- Discussing the results of a co-design process with novice developers to identify potential enhancements for the PbD prototype tool as a privacy education tool. The co-design process allowed for collaborative exploration of the tool's capabilities and limitations, leading to insights into its improvement as an educational tool.

Paper structure. The paper is structured into sections as follows: In section 2, we show related work and background information about privacy law and its challenges and the proposed solutions. Section 3 defines the methodology for enhancing and evaluating PARROT. Sections 4 and Section 5, illustrate the updated architecture of the privacy-aware interaction tool PARROT and then evaluates the tool and lists the findings and lesson learned. Section 7 concludes the study.

2 BACKGROUND AND RELATED WORK

2.1 Privacy Laws and Measures

In general, "*data privacy*" refers to the protection of individually identifiable data. It is an individual's right to control and influence the collection, storage, and disclosure of their personal information [62]. Lack of data privacy may lead to individuals having their personal data and information disclosed without their permission. In reality, data subjects could lose control over their data, such as when they are located on a server operated by a third party [3]. Many countries require compliance with data protection regulations and privacy laws, including the California Consumer Privacy Act in the United States, and the Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada, among others [67]. Similarly, the General Data Protection Regulation (GDPR) that was introduced by the European Union (EU) in 2018, confirms the importance of applying privacy principles to all systems that deal with personally identifiable components [6]. Under GDPR, organisations must obtain individuals' explicit consent before collecting, processing, or sharing any personal data. Nevertheless, individual data may not cause privacy breaches or leaks on their own. However, multiple such information may be a problem; and it is one of the major concerns with IoT devices and applications where IoT devices analyse and share sensitive data, making them vulnerable to attacks [58].

Researchers have advocated techno-regulatory approaches for minimizing and avoiding privacy risks in data processing systems. In the context of privacy-by-design (PbD) principles, these approaches are commonly referred to as privacy-enhancing technologies (PETs). Despite the fact that PbD has been proposed as a solution, the transition from a design (in which privacy requirements for an information system have been identified) to an implementation that satisfies those requirements is a challenging aspect. The key challenge is aligning design-stage privacy requirements with PETs during implementation, as well as software engineers' lack of a thorough understanding of PETs [19]. In order to address this issue, privacy patterns have been presented since patterns have served to resolve specific issues for many years.

A privacy pattern is a design pattern used in software design to describe known solutions and best practices for design problems. Initially, patterns were developed to address security issues by Yoder and Baraclow who were the first to develop information security pattern solutions [69]. In spite of some contributions not using the term "privacy pattern," it has gained increasing attention as the privacy concept has gained importance [49]. For example, Graf et al. presented the development of User Interface Patterns for Privacy Enhancing Technologies (PET) [27]. Romanosky et al. identify three privacy patterns related to web-based activities while Schemmer presents six patterns for filtering personal information [56, 61]. It is noted by Doty and Gupta that there is a lack of guidance for software engineers on how to implement Privacy-by-Design [20]. As a result, they supported a collaborative effort to develop privacy patterns. To this end, there are two websites that have been built as a collaborative work to collect and develop privacy design patterns based on software engineering design patterns[1] [2]. Despite all the efforts made towards privacy patterns, they are still not accessible to many software developers, as many of them find them difficult to understand. However, they could be easy to implement, whereas guidelines are available. Thus, it is necessary to simplify and nudge developers to incorporate privacy patterns when designing applications. Visualizing privacy may assist software developers in determining what kind of privacy-preserving measures are needed [2].

2.2 Privacy Awareness

The concept of privacy awareness refers to the understanding of how personal data is gathered, used, and protected [53]. Numerous methods exist for improving privacy awareness among software developers, including training and educating developers on privacy legislation such as GDPR, encouraging developers to make a priority for accountable privacy decisions at an early stage of the software life cycle, supporting the use of privacy-enhancing technologies such as encryption and anonymization, and promoting collaboration between the development and professional privacy teams to ensure that privacy requirements are well understood and incorporated into SW design and development. Some organizations, especially small ones, cannot provide extensive training and education on privacy issues. In addition, hiring privacy experts to work with the development team is not an option due to limited resources. Moreover, implementing privacy-enhancing technologies like encryption and anonymization can be challenging, especially for developers without technical

[1] https://privacypatterns.org
[2] https://privacypatterns.eu/

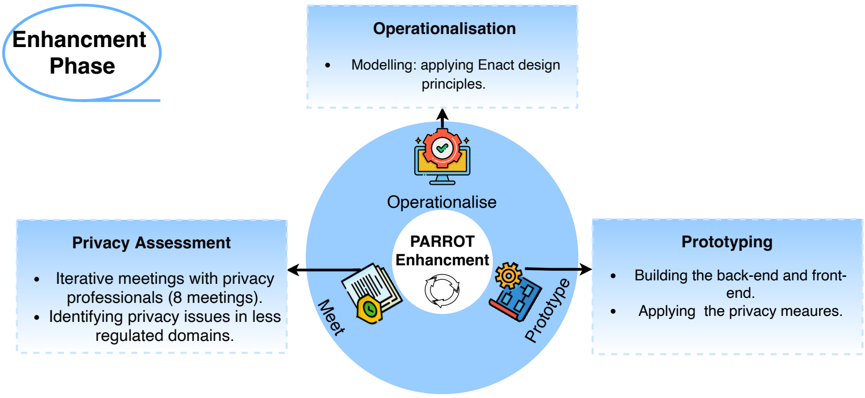

Enhancment Phase
Operationalisation
Modelling: applying Enact design principles.
Operationalise
PARROT Enhancment
Privacy Assessment
Iterative meetings with privacy professionals (8 meetings).
Identifying privacy issues in less regulated domains.
Meet
Prototype
Prototyping
Building the back-end and front-end.
Applying the privacy meaures.

Fig. 1. A requirement-gathering process that is used to extract elements to be implemented in the PbD tool for less regulated domains. In the operationalisation process, we have followed Enact design principles [39].

expertise [2]. Additionally, people do not have the memory capacity to remember all the laws and regulations concerning privacy, particularly non-privacy experts [53].

Many research efforts have been conducted to find out how to improve users' awareness. As an example, Lin [43] presents a privacy model named *privacy as expectation*. In this model, a privacy summary interface is provided to highlight both the use of sensitive resources and people's perceptions of how the app behaves. The researchers evaluated users' privacy awareness by counting the number of participants who stated privacy concerns when defending their recommendations. To address the issue of data leaks from Android phones and to raise awareness of the consequences of such leaks, Balebako et al. [7] presented a *Privacy Leaks* prototype using Just-in-Time notifications (JIT) and a summary visualization. A number of privacy tools were proposed for web browsers, including *NoTrace* [44] and *The Wi-Fi Privacy Ticker* [15], to provide users with information that they can use to make informed decisions about their privacy. *FoxIT* [25] and *PScore* [52] are also proposed as enhancing tools for users' privacy and security awareness and behaviour in mobile apps and online social networks.

Taking into account these tools, it is evident that a visual tool may be able to educate users and assist them in making informed decisions regarding privacy and security. We propose a prototype tool, PARROT, which targets software developers who have responsibility for augmenting privacy features into IoT designs, on which the suggested guidelines are difficult to translate [65]. It supports interactive and easy-to-follow techniques which are presented in a simple, explicit and straightforward way [2]. Using such a tool could help novice developers and university students to become more privacy-aware.

3 METHODOLOGY

We have constructed our approach in two phases enhancement and evaluation phases, as shown in Figures 1 and 2. As part of the first phase, we intend to enhance the tool's ability to incorporate more privacy features. In our initial work [2], we have worked on different IoT use cases, such as health-related applications, smart homes, and bus routing. However, health-related ones are well-regulated domains. Although online pharmacy, which we use in this study, falls within the health domain, it has some privacy challenging aspects that could have different legal interpretations, such as social plug-ins, profiling, and online payment, that we have discussed in Section 4.1.

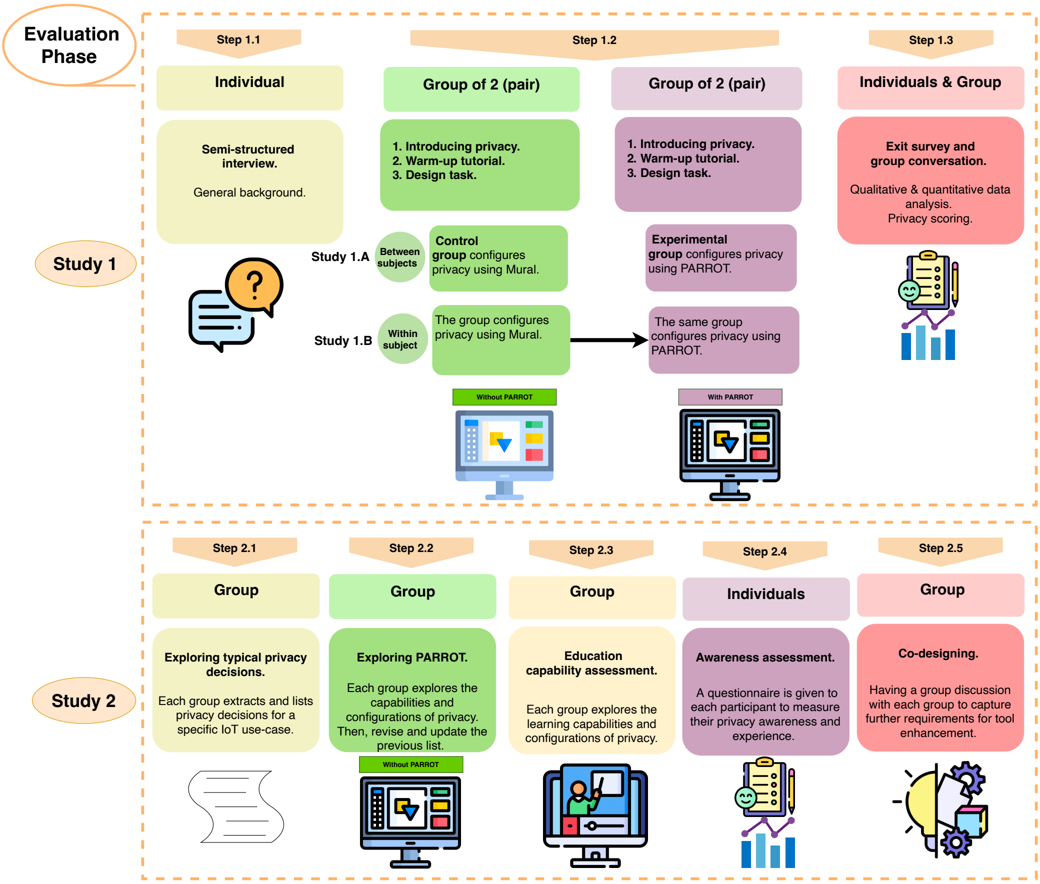

Evaluation Phase
Study 1
Step 1.1
Individual
Semi-structured interview.
General background.
Step 1.2
Group of 2 (pair)
1. Introducing privacy.
2. Warm-up tutorial.
3. Design task.
Group of 2 (pair)
1. Introducing privacy.
2. Warm-up tutorial.
3. Design task.
Study 1.A
Between subjects
Control group configures privacy using Mural.
Experimental group configures privacy using PARROT.
Study 1.B
Within subject
The group configures privacy using Mural.
The same group configures privacy using PARROT.
Without PARROT
With PARROT
Step 1.3
Individuals & Group
Exit survey and group conversation.
Qualitative & quantitative data analysis.
Privacy scoring.
Study 2
Step 2.1
Group
Exploring typical privacy decisions.
Each group extracts and lists privacy decisions for a specific IoT use-case.
Step 2.2
Group
Exploring PARROT.
Each group explores the capabilities and configurations of privacy. Then, revise and update the previous list.
Without PARROT
Step 2.3
Group
Education capability assessment.
Each group explores the learning capabilities and configurations of privacy.
Step 2.4
Individuals
Awareness assessment.
A questionnaire is given to each participant to measure their privacy awareness and experience.
Step 2.5
Group
Co-designing.
Having a group discussion with each group to capture further requirements for tool enhancement.

Fig. 2. The evaluation process which is discussed in detail in Section 5. The evaluation consists of two main studies: **Study 1** focuses mainly on assisting to design privacy-aware IoT applications for less regulated domains, while **Study 2** focuses on educating novice developers.

During the first phase, explained in Section 4, we have expanded the prototype by adding other components that trigger privacy threats. In order to make sure that the tool is better compliant with privacy laws, we worked iteratively with a privacy lawyer. In addition, we validated the privacy fulfilment with other privacy professionals to minimise any subjectivity that could be caused. The second phase aims to evaluate what we have implemented in the first one using two separate lab studies that are explained in Section 5.

In our approach, we adopted the co-design method. We actively involve stakeholders in the design process to ensure that the final product fits their requirements and is practical. Detailed explanations of this approach will be provided in Sections 4 and 5. Our focus here is primarily on addressing the following key research questions:

- (**RQ1**) *Does the tool help to design privacy-aware IoT applications for less regulated domains as highly regulated domains?*
- (**RQ2**) *Does the tool help increase awareness about laws and privacy-preserving measures, such as privacy patterns, among software developers?*

Table 1. Use-case scenario description in which the prototyping and evaluation phases are based.

Scenario 1: Online pharmacy
Consider a user who accesses a cloud-hosted online pharmacy to place an order, pay, and get a prescription delivered to their home. This involves a variety of different parties receiving the personal data of the user depending on their role – the pharmacy, payment provider, delivery company, and cloud hosting service used by the pharmacy to host and manage its website and mobile app. In addition to these parties, the pharmacy increases its revenue by including social media plugins and online marketing on its website and mobile app. The marketing uses real-time bidding (RTB) to offer the advertising inventory space. As a result, more parties process the user's personal data. Each party processes a different set of the user's personal data for a different purpose either as a controller or the processor.
Scenario 2: Smart home
Consider a service that aims to build a smart home app. In this use case, the smart home has four sensors: thermostat, light, camera, and car lock. The app's primary purpose is to control all these sensors, such as opening the car door lock or truing the light on/off when the user wants. The data transfers back and forth between the sensors to the cloud to the phone app. In this app, we aim to control the sensor on the stated purpose of each one of the sensors while keeping the client's privacy protected.

- (**RQ3**) *Does the tool be able to educate novice developers about privacy-preserving measures and laws?*
- (**RQ4**) *Are there any ways to enhance the privacy learning experience for users through co-design with novice developers?*

4 PHASE 1: ENHANCEMENT

The *Enhancement Phase* of our work aimed to investigate additional privacy concerns and evaluate the scalability of the tool across different domains, less regulated once specifically. We started with the Continuous Glucose Monitoring (CGM) use case which is in a well-regulated domain (health data)[2]. Here we look in depth at less-regulated domains such as online pharmacy [8] and smart home to uncover further privacy issues. The process was performed iteratively, incorporating privacy measures (privacy patterns) and testing the prototype with privacy professionals to confirm GDPR compliance.

Despite the fact that the CGM use-case presented significant privacy pitfalls [2], health data is considered as a well covered domain when it comes to privacy GDPR compliance [21]. In this process, we aim to enhance our prototype tool by adding additional aspects that could create privacy pitfalls, such as online payment and social plug-ins. Initially, we started with one use-case, i.e. online pharmacy, since single case studies are very effective in research when a comprehensive understanding of the phenomenon is required [1]. Scholars have suggested that starting with a single case study allows the researcher to evaluate established theoretical linkages and investigate new ones [68]. Upon further consideration, we introduced a second use-case (smart home) in order to identify any privacy concerns that may have been overlooked.

4.1 Complexity in Less Regulated Domains

Despite the importance of such principles and measures, applying privacy could be challenging especially for less regulated domains. To illustrate the privacy challenges for less regulated domains, we presented a multi-cloud online pharmacy scenario as stated in Table 1. In the online pharmacy use case, we have multiple components to consider, such as third parties (Cloud4U), use of subcontractors (payment and shipping providers), use of social plug-ins on the website (Friendface). Three key issues relating to online pharmacy is listed as follows: using a social plug-in which leads to *cookie placement*, *profiling by Friendface*, and using *real-time bidding*. In addition, there are many technologies are involved in this scenario that raise privacy concerns such as *Adtech*. In the subsequent discussion, we will explore each challenge in more detail to provide a better understanding.

Adtech. Before discovering the privacy risks associated with the online pharmacy components, this field is known as Advertising technology (Adtech), which refers to the tools and software that advertisers employ to reach audiences, deliver, and measure digital advertisements. Many data protection regulators are intensely interested in this field [10, 24, 66]. For instance, the Information Commissioner's Office (ICO), UK regulator, issued an opinion on it in November 2021 about data protection standards that corporations developing new advertising technologies (Adtech) must follow to preserve people's privacy online [32]. Even with privacy notices and individuals exercising rights, the ICO considers the data sharing required to implement Adtech solutions to be excessive and not something that individuals can completely comprehend or control. In the same way, some technological developments have been expected to impact how Adtech and its revenue will operate in the future. This is exemplified in work undertaken by Apple's Identifier for Advertising and App Tracking Transparency framework [5]. Google's Advertising ID for Android is also another example of these technological developments, as it allows users to opt-out of interest-based ads generated via profiling [26].

Cookies. Placing social plug-ins leads to cookie placement, which is governed by two parts of legislation. The first is the e-Privacy Directive (2005/58/EC) as implemented into national law. In the UK, this is the Privacy and Electronic Communications (EC Directive) Regulations 2003. The second legislation is that cookies and their equivalents can only be placed with active consent, which GDPR regulates. In our previous work, we did not investigate the cookies and their regulation. Therefore, it is one of the aspects we are trying to capture into PARROT. Figure 3 shows that cookies placement (i.e., necessary, analytical, and ad/targeting cookies) triggers three privacy requirements: having a surface cookies banner, capturing consents or acceptance, and placing cookies based on the consent. In case of using the necessary cookies only, having a surface cookies banner is sufficient to comply with the privacy requirements regarding cookies placement. It is worth noting that cookie banner must be able to be resurfaced if a new cookie is added, or the website permits cookies to be placed by third parties, then a change in the third-party placement of cookies will also require the banner to be resurfaced. In addition, the cookie banner must be resurfaced to remove existing cookies if browser settings have changed. Whilst the tool includes cookies to notify the developer about their existence, we consider giving the developers some examples of the two key providers of cookie consent solutions, such as OneTrust (cookiepro.com) and TrustArc (trustarc.com).

Profiling . Another significant aspect of issues relating to the online pharmacy is using profiling (i.e. Friendface). Profiling, which is regulated by GDPR (Arts 21 and 22), can broadly be defined as creating a social media users' profile using their social data [9, 36]. Friendface uses this information for patient's profile enrichment (profiling), which is useful for its advertising business. This has also been seen in the case of Facebook's connections targeting and Automated App Ads tools [45, 46]. Similarly, Google also offers a variety of online advertising products (ads.google.com). The use of profiling in IoT apps, such as health apps, raises privacy concerns regarding the possibility of malicious activities exploiting user data [59]. Profiling-related issues can be minimised and user data can be protected by prioritising privacy and security measures. The key impact for software developers, while using PARROT, would be to ensure that the software is able to accommodate requests from the users (data subjects) to stop processing their personal data.

Real-time bidding. In addition to using social plug-ins and profiling, real-time bidding (RTB) is another key issue in the use case. RTB is one of the important concepts in display advertising, also known as programmatic buying, in which advertisers have the option to make decisions for each impression (auction) [70]. The privacy point here is sharing the customer's personal data with numerous third parties, resulting in a complex supply chain that is difficult to control, difficult to ensure processing personal data securely, and difficult to pass on the user's data rights requests when made (e.g., stopping processing).

4.2 Compartmentalisation

We applied a compartmentalisation approach by introducing one component at a time and evaluating potential privacy concerns. This phase is performed iteratively with a privacy lawyer since the merging of components may create more complex privacy issues that developers must consider when designing IoT apps. Moreover, we incorporated privacy measures, i.e. privacy patterns, to promote privacy compliance and eliminate specific privacy vulnerabilities [40]. During our investigation of the tool's scalability to multiple domains, we observed some of the challenges.

Having many different interpretations of GDPR policies, which is a major challenge. For example, two components are classified in the online pharmacy use case as subcontractors. One is a payment provider, while the other is a shipping provider. Nevertheless, in Masoud et al [8], only the online pharmacy is considered a data controller, and all other cloud components are considered data processors. According to a privacy lawyer who has reviewed this issue, this is not the case. "*My experience of these types of third parties is that they are not automatically processors*", the lawyer states. For instance, the shipment company holds personal data, such as name and address, for tracking services which entitle the company to be a data controller [33]. On the other hand, postal services neither can be controllers nor processors without a tracking aspect. In addition to the shipment company, the payment company is usually a data controller on the basis that the website user is directed to the payment provider's web-page for payment and the retailer (the online pharmacy) does not collect or process any payment information [33].

Therefore, after integrating all the components, we tested the prototype with two privacy specialists to confirm GDPR compliance. This led us to construct an enhanced high-level flowchart diagram, illustrated in Figure 3, which aims to apply privacy techniques to the proposed use-cases, which can be used as the basis for the development of PARROT as well as to visualize the app's design components using Enact's design principles [39]. PARROT interface represents the main feature is illustrated in Figure 4.

5 PHASE 2: EVALUATION

Our evaluation was based on the application of use-cases, which was influenced by similar techniques such as LINDDUN and Coconut [17, 41, 50]. Our main goal is to explore the capabilities of the tool to supplement privacy measures in less regulated domains and increase privacy awareness among software developers. In particular, our objective is to answer the following research questions (RQ1-RQ4).

Using a qualitative and quantitative research approach, we were able to gain a deeper understanding of developers' design practices while evaluating the tool's effectiveness. In order to avoid biasing the sample, we did not refer to privacy or security during the recruitment process [44]; rather, we simply explained that we were searching for participants who were interested in participating in an evaluation research project. We used methods such as randomization and partial blinding to

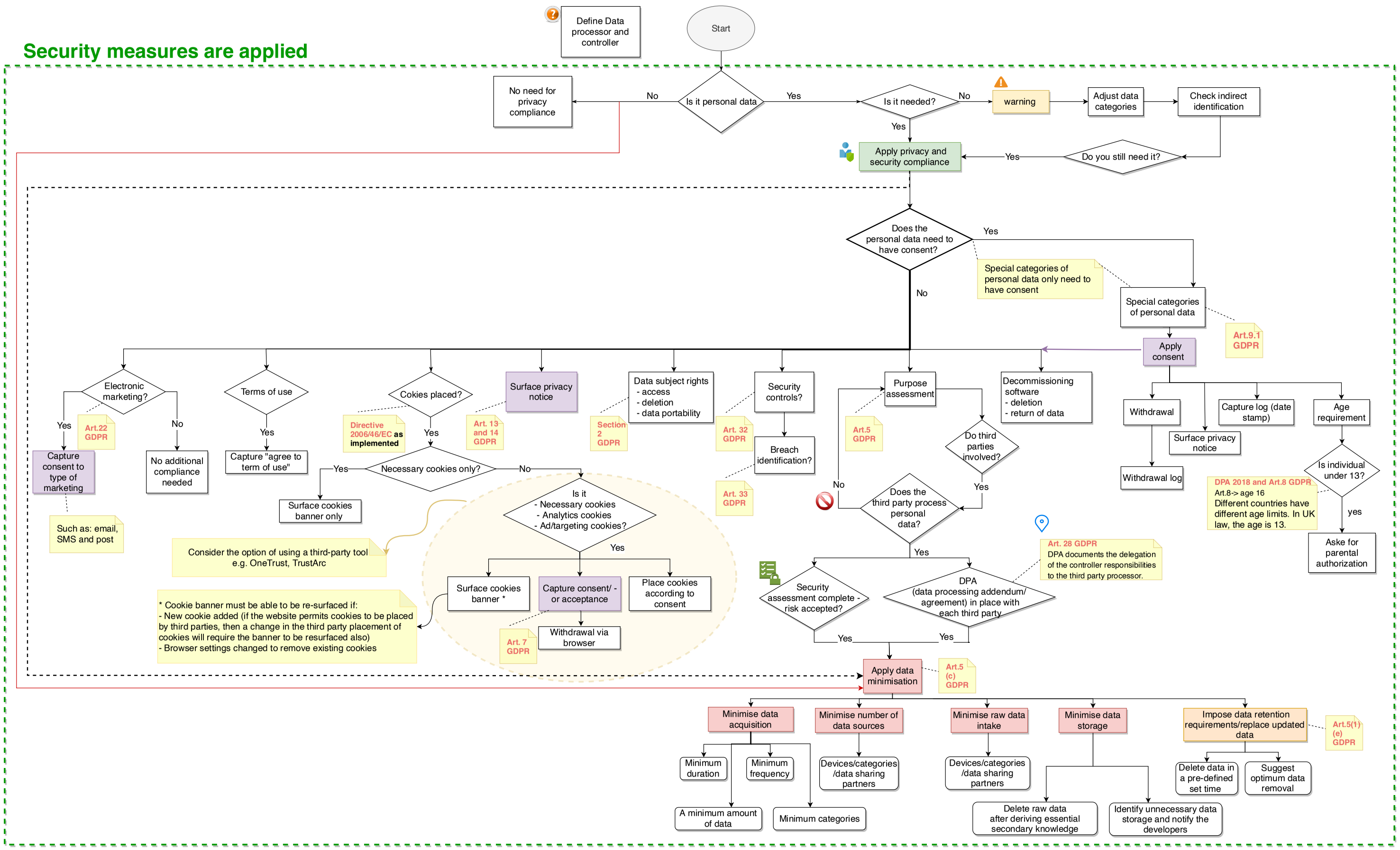
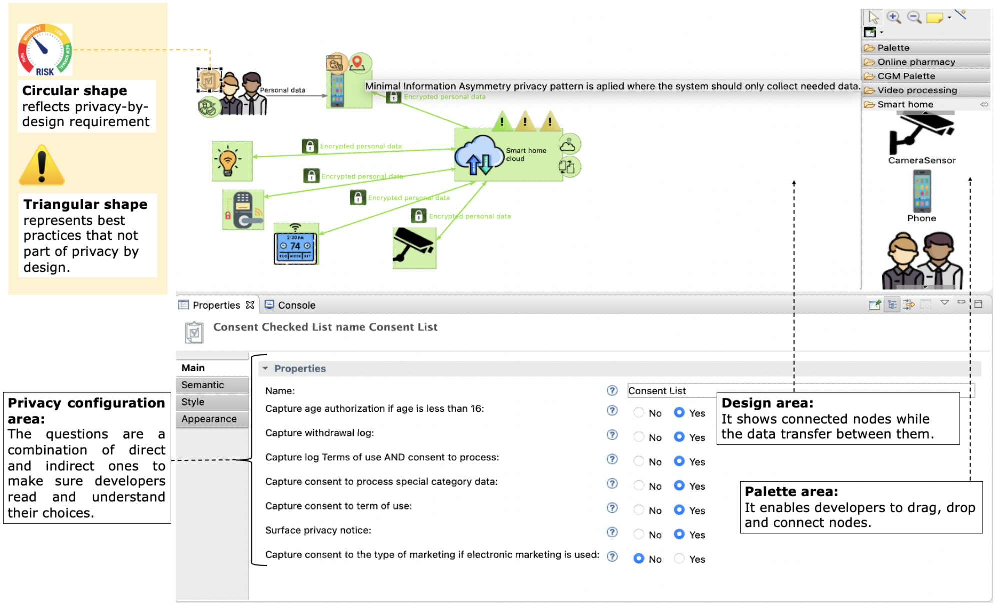

Security measures are applied
Define Data processor and controller
Start
Is it personal data
No
No need for privacy compliance
Yes
Is it needed?
No
warning
Adjust data categories
Check indirect identification
Do you still need it?
Yes
Yes
Apply privacy and security compliance
Does the personal data need to have consent?
Yes
Special categories of personal data only need to have consent
Special categories of personal data
Art.9.1 GDPR
Apply consent
Withdrawal
Withdrawal log
Surface privacy notice
Capture log (date stamp)
Age requirement
Is individual under 13?
DPA 2018 and Art.8 GDPR
Art.8-> age 16
Different countries have different age limits. In UK law, the age is 13.
yes
Aske for parental authorization
No
Decommissioning software
- deletion
- return of data
Purpose assessment
Art.5 GDPR
Do third parties involved?
Yes
No
Does the third party process personal data?
Yes
Art. 28 GDPR
DPA documents the delegation of the controller responsibilities to the third party processor.
DPA
(data processing addendum/ agreement) in place with each third party
Security assessment complete - risk accepted?
Yes
Yes
Apply data minimisation
Art.5 (c) GDPR
Security controls?
Art. 32 GDPR
Breach identification?
Art. 33 GDPR
Data subject rights
- access
- deletion
- data portability
Section 2 GDPR
Surface privacy notice
Art. 13 and 14 GDPR
Cookies placed?
Directive 2006/46/EC as implemented
Yes
Necessary cookies only?
Yes
No
Surface cookies banner only
Is it
- Necessary cookies
- Analytics cookies
- Ad/targeting cookies?
Yes
Surface cookies banner *
Capture consent/ - or acceptance
Place cookies according to consent
Withdrawal via browser
Art. 7 GDPR
Consider the option of using a third-party tool e.g. OneTrust, TrustArc
* Cookie banner must be able to be re-surfaced if:
- New cookie added (if the website permits cookies to be placed by third parties, then a change in the third party placement of cookies will require the banner to be resurfaced also)
- Browser settings changed to remove existing cookies
Terms of use
Yes
Capture "agree to term of use"
Electronic marketing?
Art.22 GDPR
Yes
Capture consent to type of marketing
Such as: email, SMS and post
No
No additional compliance needed
Minimise data acquisition
Minimum duration
Minimum frequency
A minimum amount of data
Minimum categories
Minimise number of data sources
Devices/categories /data sharing partners
Minimise raw data intake
Devices/categories /data sharing partners
Minimise data storage
Delete raw data after deriving essential secondary knowledge
Identify unnecessary data storage and notify the developers
Impose data retention requirements/replace updated data
Art.5(1) (e) GDPR
Delete data in a pre-defined set time
Suggest optimum data removal

Fig. 3. An enhanced high-level flowchart diagram for devising the PARROT prototype tool.



Circular shape reflects privacy-by-design requirement

Triangular shape represents best practices that not part of privacy by design.

Privacy configuration area: The questions are a combination of direct and indirect ones to make sure developers read and understand their choices.

Design area: It shows connected nodes while the data transfer between them.

Palette area: It enables developers to drag, drop and connect nodes.

Consent Checked List name Consent List

Properties

Name: Consent List

Capture age authorization if age is less than 16: ○ No ● Yes

Capture withdrawal log: ○ No ● Yes

Capture log Terms of use AND consent to process: ○ No ● Yes

Capture consent to process special category data: ○ No ● Yes

Capture consent to term of use: ○ No ● Yes

Surface privacy notice: ○ No ● Yes

Capture consent to the type of marketing if electronic marketing is used: ● No ○ Yes

Fig. 4. A PARROT interface represents the main features, including simplified visual notation, privacy configuration area, pallet area, and design area. The details of the interface are provided in [2].

minimize the impact of any bias that might have been present [37]. During the between-subject studies, participants were randomly assigned to either the control group or the treatment group [37]. During the evaluation, we implemented a strict procedure to ensure that each participant received the same level of attention to minimise the likelihood of differential behaviours [23]. The evaluation consists of two main studies, where **Study 1** is focused on addressing RQ1 and RQ2, while **Study 2** focuses on addressing RQ3 and RQ4.

5.1 Study 1 Design

The analysis presented here is based on two lab controlled studies (A and B). To test RQ1 and RQ2, we have applied two evaluation techniques which are between-subject evaluation and within-subject evaluation for two different use-cases. In **Study 1.A**, a between-subjects evaluation was performed to minimize any potential individual learning effects. Furthermore, we performed a within-subject evaluation in **Study 1.B** to reduce individual variation in Study 1.A as well as to compare different participant designs using different design tools. For both studies, participants worked in pairs since software design is typically a collaborative activity [14]. Each study session lasted between 1.5-2 hours.

5.1.1 ***Recruitment***. We recruited participants through the university email group targeting university students (undergraduate (UG), postgraduate (PG) taught and PG Research in computer science) who have worked on IoT applications for at least a year [30]. Those who agreed to participate in the study and were eligible were recruited and given consent forms. Upon completion of the study, participants received vouchers for £20. The undergraduate novice developers were enrolled in two modules: Network Communication and Group Project. Among the participants, five of them are full-stack developers, and six are actively working on IoT development projects.

Table 2. Twenty privacy patterns applied to the tested use cases. The patterns are picked based on their applicability to the use cases. Sources: (privacypatterns.org) and (privacypatterns.eu)

Privacy patterns	
1. Use of dummies	11. Data breach notification
2. Location granularity.	12. Privacy dashboard
3. Minimal information asymmetry	13. Added-noise obfuscation
4. Asynchronous notice	14. Increasing aggregation awareness
5. Privacy policy display	15. Privacy awareness panel
6. Outsourcing [with consent]	16. Obtaining explicit consent
7. Onion routing	17. Informed implicit consent
8. Anonymity set	18. Who's listening
9. Pseudonymous identity	19. Sticky policies
10. Privacy icons	20. Lawful consent

5.1.2 ***Evaluation sessions.*** **Study 1.A** intends to assess whether PARROT developers are capable of creating IoT designs that preserve privacy more effectively. Therefore, we randomly assigned 16 participants to one of two conditions (using or not using the PARROT tool). The participants were divided into two groups, an experimental group (E) and a control group (C). Each group consisted of eight participants; in both groups, participants worked in pairs. At the beginning, both groups were given 20 minutes introduction to privacy, followed by a tutorial on Mural for *Group C* only and PARROT for *Group E* only. We presented two videos [3][4] about privacy and its issues produced by Privacy International [5] to maintain consistency and accuracy. Following this, participants were provided with a list of 20 privacy patterns based on their applicability to the use case (Table 2).

Control group (C) was asked to design a smart home scenario using the Mural tool (see Table 1), while applying privacy by design concepts and privacy patterns, as seen in Figure 5. In the *experimental group (E)*, the same task was performed using the PARROT tool. Following the session, both groups were asked to complete a ten-minute exit questionnaire.

Study 1.B was conducted with 10 participants (5 groups working in pairs). All the participants completed a design task for the online pharmacy app (see table 1) once using Mural and then once using PARROT. We aim to test whether the tool helps them increase their knowledge of privacy principles and privacy patterns. To achieve this, we conducted the study in three rounds. ***Round 1 (No privacy using Mural)***: participants were asked to do IoT application design without training, guidance, or reference to privacy or its patterns. For each pair, we prepared a Mural link where they can draw IoT application designs related to the use case. ***Round 2 (With privacy using Mural)***: the participants were provided with a 20-minute introduction to privacy and privacy patterns (similar to Study 1.A).

Afterwards, we provided participants with a list of 20 privacy patterns and explained how to use them. In order to distinguish between the different design activities of each round, we asked participants to use different colours and sticky notes. As a next step, they had to complete a questionnaire. ***Round 3 (With privacy using PARROT):*** this round is similar to round two, except that PARROT was used instead of Mural. Prior to performing the design task, participants were trained in the use of PARROT. Finally, they had a ten-minute exit questionnaire.

[3] What Is Privacy? https://youtu.be/zsboDBMq6vo

[4] Data Protection Explained https://youtu.be/VUae3XgIZVU

[5] https://www.privacyinternational.org

Table 3. A privacy by design scorecard was developed by the privacy lawyer for use in scoring the designs produced by developers. Note: PD means Personal Data.

Principle	Explanation	Score
1: Privacy requirements intrinsic in design and analysis.	Understand and commit to privacy as BAU practice rather than as compliance add-on.	3
2: Privacy embedded in the design.	Ensure privacy is integral to the architecture without impairing functionality being.	3
3: Full functionality.	Privacy is valued alongside the other aspects of the project: design, objectives, security, third parties etc.	3
4: End-to-end security.	Lifecycle protection of the data (including PD) - collection, use, disclosure, retention, and deletion.	3
5: Visibility and transparency.	End-user trust: accountability, openness, and compliance.	3
6: Respect for User Privacy.	All PD belongs to the end user, not to us. Respect for and understanding of this principle support the implementation of functionality that enables end-user to understand PD processing and access their PD.	3
		18

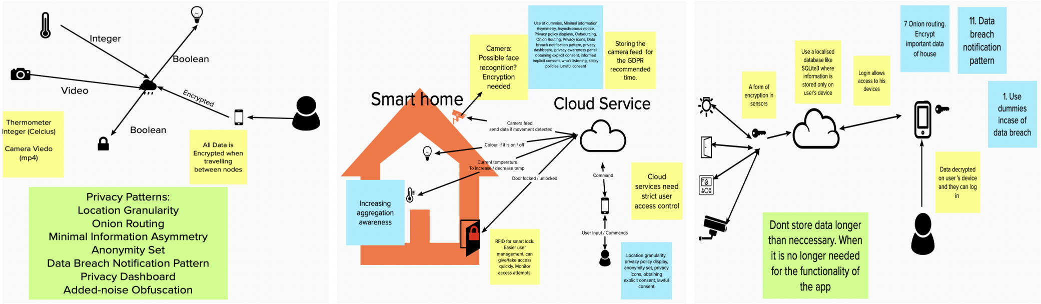

Integer
Boolean
Video
Encrypted
Boolean
Thermometer
Integer (Celcius)
Camera Viedo
(mp4)
All Data is Encrypted when travelling between nodes
Privacy Patterns:
Location Granularity
Onion Routing
Minimal Information Asymmetry
Anonymity Set
Data Breach Notification Pattern
Privacy Dashboard
Added-noise Obfuscation
Camera: Possible face recognition? Encryption needed
Use of dummies, Minimal information Asymmetry, Asynchronous notice, Privacy policy displays, Outsourcing, Onion Routing, Privacy icons, Data breach notification pattern, privacy dashboard, privacy awareness panel, obtaining explicit consent, informed implicit consent, who's listening, sticky policies, Lawful consent
Storing the camera feed for the GDPR recommended time.
Smart home
Cloud Service
Camera feed,
send data if movement detected
Colour, if it is on / off
Current temperature
To increase / decrease temp
Door locked / unlocked
Command
User Input / Commands
Cloud services need strict user access control
Increasing aggregation awareness
RFID for smart lock. Easier user management, can give/take access quickly. Monitor access attempts.
Location granularity, privacy policy display, anonymity set, privacy icons, obtaining explicit consent, lawful consent
A form of encryption in sensors
Use a localised database like SQLite3 where information is stored only on user's device
Login allows access to his devices
7 Onion routing. Encrypt important data of house
11. Data breach notification pattern
1. Use dummies incase of data breach
Data decrypted on user 's device and they can log in
Dont store data longer than neccessary. When it is no longer needed for the functionality of the app

Fig. 5. Participants' design tasks Using MURAL for 3 different pairs. In the left and middle samples, the participants tend to apply the privacy patterns without specifying where they could be applied. In the right picture, the participants attempted to apply the patterns at several locations.

Data collection and scoring. Data was collected using video and audio recordings for qualitative research purposes. We ended up with 13 designs and 26 scoring sheets. Each design was scored according to the six privacy principles listed in Table 3. In addition, they were scored based on 20 privacy patterns listed in Table 2. To evaluate the overall score of the privacy principle, the lawyer assigned a score for each principle as 3: if privacy is considered, the issue is identified, and the solution is correct; 2: if privacy is considered and the issue is identified; 1: if privacy is considered; and 0: no privacy. As well as the overall privacy principle score, we assign a mark for each privacy pattern as 2: privacy pattern considered in a reasonable place; 1: if privacy pattern considered overall, but not in a reasonable place; 0: if no pattern consideration is made. An expert on privacy patterns was consulted to reduce the basis of the researchers.

5.2 Study 2 Design

5.2.1 ***Recruitment.*** 16 participants were recruited through the university email group targeting university students (UG, PG taught and PG Research in computer science). In order to avoid a biased sample, we did not mention privacy, privacy threats, or concerns during recruitment; rather, we simply stated that we were looking for individuals interested in participating in an evaluation study. Upon completion of the study, participants received vouchers for £25.

5.2.2 ***Procedure.*** This controlled lab study consists of five different phases in which we carried out the following steps: *privacy decision exploration, PARROT tool exploration, education capability assessment, awareness assessment,* and finally, *co-designing*. In the first phase, we showed the participants an introductory video about privacy [6]. The purpose of this exercise is to stimulate their thinking about privacy and to assist them in recalling their previous experiences and knowledge of privacy. Then, we gave each group two IoT use-cases (CGM and smart home [2]) and asked them to extract and list all the privacy decisions for the given IoT use-case. Specifically, we asked them to explain how they think privacy works in these apps and explain why they made these decisions. After that, we gave them a brief tutorial about PARROT and let them explore the tool and observe the privacy capabilities and configuration by themselves. Additionally, we provided them with a list of 20 privacy patterns that are applicable to the use-cases (listed in Table 2). After they had finished, we asked them to review and update their previous privacy decisions based on their own explorations and the given patterns.

In the third phase, each group was given two other use-cases (bus routing and online pharmacy) that had been pre-designed by a senior developer using PARROT. We asked them to simulate these designs and configurations into CGM and smart home use cases they had already worked on, but this time in PARROT. Once they finished simulating, they were instructed to update their previous lists and privacy patterns on paper. We were attempting to determine what privacy-preserving measures they had taken here. If, for example, the location of the cloud server has been changed after PARROT has been used. For qualitative purposes, participants need to explain how PARROT enhances privacy. Figure 6 illustrates a few examples of privacy decisions made by participants at the end of phase 3.

Following these steps, each participant was asked individually to fill out a questionnaire to measure privacy awareness and user experience. To measure the level of awareness, many researchers rely on pre- and post-questioning [29, 35]. Since we did not want to influence an individual's awareness or introduce any bias, we did not ask any privacy questions before exploring PARROT [57]. Therefore, some of the questions asked about the participant's experience and knowledge prior to and after utilizing the PARROT tool. By giving them privacy questions prior to using the tool, their thinking would be influenced to focus on these aspects. It is therefore difficult to assess whether privacy knowledge has increased through the use of the tool or otherwise.

[6] What Is Privacy? https://youtu.be/zsboDBMq6vo

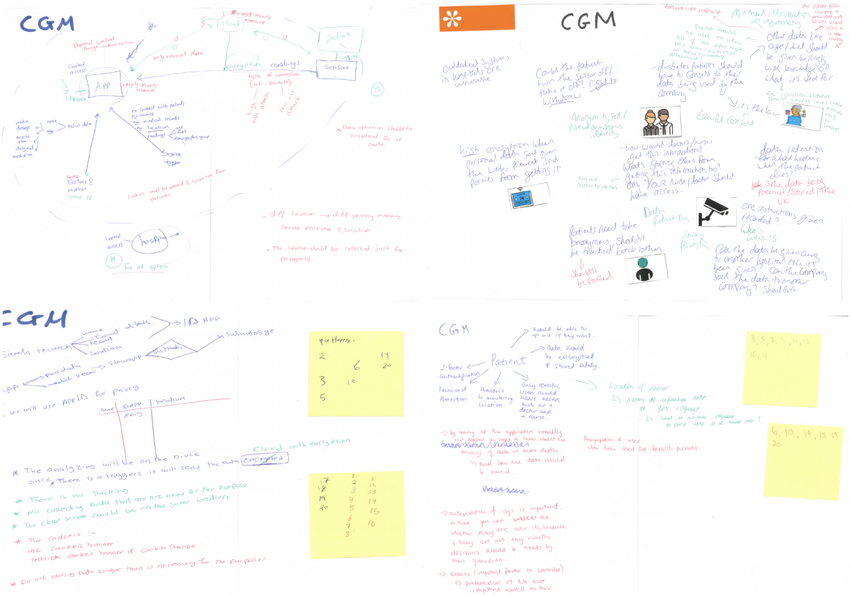


Fig. 6. Participants' design tasks illustrate a variety of approaches used by them to express their approach to privacy decisions. Besides the data flow diagram, participants also used icons, lists, and detailed text descriptions. For each phase, participants were instructed to use a different colour. Phase one, two and three are represented by the colours blue, green and red respectively.

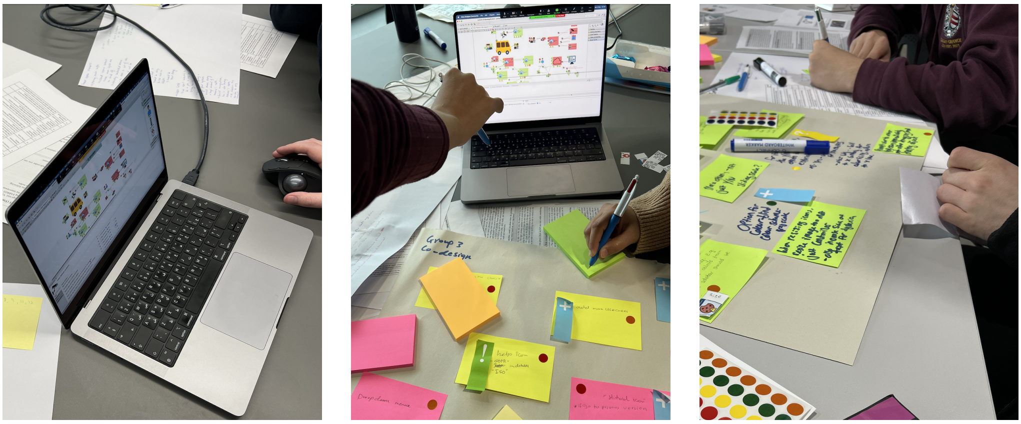


Fig. 7. **Left:** Participants simulate pre-designed IoT apps in order to gain an understanding of their privacy properties. **Middle:** Participants interact with the existing privacy-by-design application tool (PARROT) during the Co-design phase. **Right**: Discussion between participants regarding how PARROT may be enhanced during the Co-design phase.

The tool might help novice developers incorporate privacy into their designs. Nevertheless, it sometimes does not specify exactly what and how privacy can be addressed, especially for novice users such as students. Accordingly, each group spent 30 minutes brainstorming possible enhancements they would like to make to the PARROT tool, as seen in Figure 7. Our goal is to explore additional requirements that support teaching privacy. In order for the tool to be an

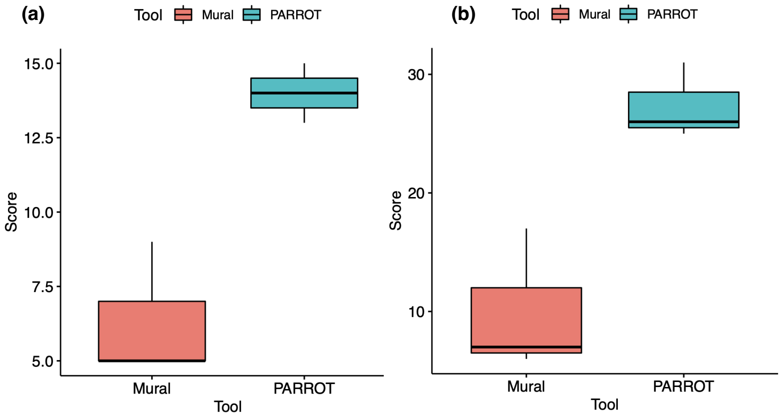


Fig. 8. (a) Mean rates of privacy principles scores for both the control group (using MURAL) and experimental group (using PARROT). (b) Mean rates of privacy patterns in Mural and PARROT. Both (a) and (b) are used for the smart home use-case.

educational tool for privacy, what aspects must it have? How would this tool help novice developers learn about privacy and the law?

6 FINDINGS AND RESULTS

6.1 Quantitative analysis

6.1.1 Privacy Assessment. We have followed the common analysis methods in software engineering research [63]. The Kruskal-Wallis test was used to evaluate the results of **Study 1.A** in order to determine if there was a statistically significant difference between the two groups (E and C). Both privacy principles (p-value = 0.0463 < 0.05) and privacy patterns (p-value =0.04953 < 0.05) revealed a significant difference. For the posthoc test, the Dunn Test was used to test if there is a statistical difference between Mural and PARROT. We observed a significant difference for both privacy principles (p-value=0.04630159 < 0.05) and privacy patterns (p-value =0.04953461 < 0.05), as shown in Figure 8.

For **Study 1.B**, Friedman rank sum tests showed a significant difference in privacy principles scores between the three rounds (p-value = 0.006738 <0.05). As a posthoc test, the Pairwise Wilcoxon rank sum test was used to determine if there was a statistical difference between Mural and PARROT (rounds 2 and 3). The comparison reveals that all rounds are significantly different, with the difference between round 2 and round 3 (p-value is 0.036 <0.05). A Wilcoxon test was conducted to determine whether the median privacy patterns score using Mural was lower than PARROT for the same participants. Wilcoxon test results showed a significant difference (p-value = 0.02895<0.05), with Mural producing lower privacy patterns scores than PARROT. The results for both studies are shown in Figures 9.

In **Study 2**, Friedman rank sum tests showed a significant difference in the number of privacy decisions among the three phases in the smart home use-case (p-value =0.0009119). As a posthoc test, Wilcoxon rank sum test indicates there is a statistical difference between phase 1 and phase 3 only (p-value =0.0072 < 0.05). In the CGM use case, the Friedman rank sum test reveals a significant difference in privacy decisions among all phases (p-value =0.0009119). The Wilcoxon rank sum test shows a statistical difference between phases 1, 2, and 3 (with a p-value < 0.05). The results for both use-cases are shown in Figures 10.

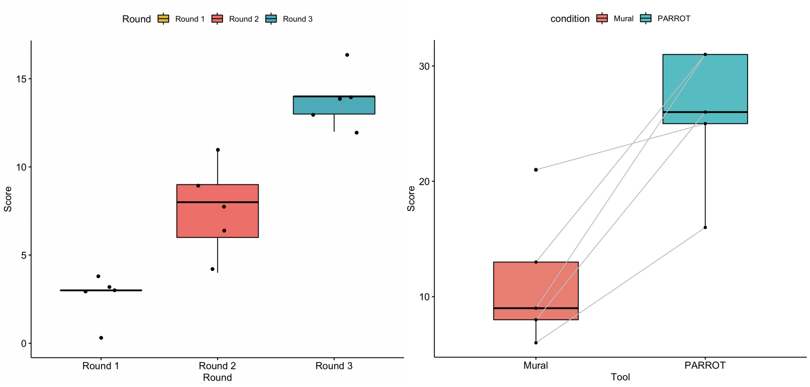


Fig. 9. (a) Mean rates of privacy principles scores for the same participants for 3 rounds. Round 1: No privacy using Mural, Round 2: With privacy using Mural and Round 3 (With privacy using PARROT). (b) Mean rates of privacy patterns in Mural and PARROT. Both (a) and (b) are used for online pharmacy use-case.

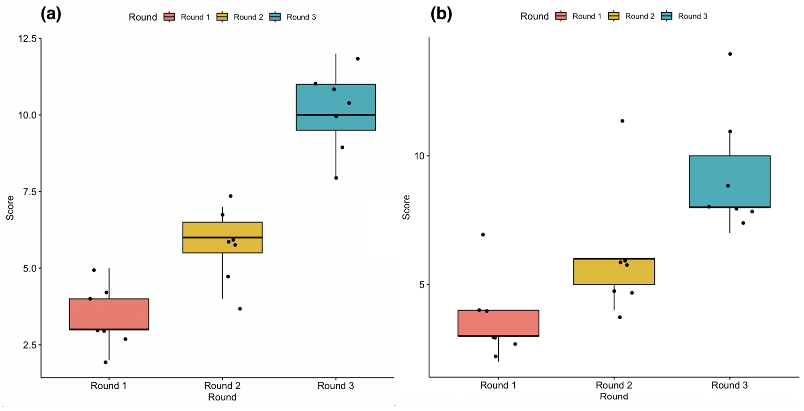


Fig. 10. Mean rates of the number of privacy decisions for the same participants over 3 phases. Phase 1: Exploring typical privacy decisions, Phase 2: Exploring PARROT, and Phase 3: Educational capability assessment. (a) Mean rates for CGM use-case. (b) Mean rates for smart home use-case.

6.1.2 The Effectiveness of PARROT. We assessed PARROT's effectiveness and usability using different key metrics from similar works, including user accuracy, user confidence, self-report scale, knowledge survey, and quality of user experience [15, 29, 35, 48, 60]. We have used a 5-point Likert scale for the factual privacy questions and general privacy self-report scale questions. For privacy patterns familiarity questions, we used a 3-point Likert scale with unfamiliar, somewhat familiar but never used, and familiar and I know where to implement it. All the questions are listed in the appendix A.

The utilisation of PARROT has shown a positive impact on participants' knowledge and understanding of privacy. In factual questions, the answers were rated on a 5-point Likert scale as: "Definitely no," "Probably no," "Unsure," "Probable yes," and "Definitely yes." To evaluate user accuracy, we counted the number of participants that correctly answered questions (Q1–Q11). Participants' answers as "Definitely yes" or "Probably yes" were coded as correct when the correct answer is yes, and "Definitely no" or "Probably no" when the correct answer is no. User confidence

	Before PARROT	After PARROT
Q1	0.75 (0.56)	1.00 (0.75)
Q2	0.44 (0.00)	1.00 (0.56)
Q3	0.63 (0.19)	0.94 (0.44)
Q4	0.81 (0.50)	1.00 (0.69)
Q5	0.38 (0.00)	0.81 (0.38)
Q6	0.44 (0.13)	0.88 (0.50)
Q7	0.19 (0.06)	0.88 (0.50)
Q8	-	-
Q9	0.19 (0.13)	0.75 (0.38)
Q10	0.19 (0.00)	0.69 (0.25)
Q11	0.19 (0.00)	0.56 (0.19)

Fig. 11. The mean accuracy rate for privacy knowledge questions in study 2. Note: Mean confidence-accuracy rates are shown in parentheses. Q8 was determined to be ambiguous and was therefore excluded from the analysis. The questions are provided in Appendix A.2

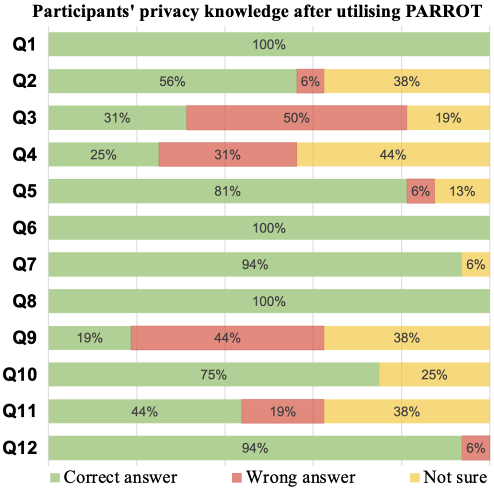


Fig. 12. A post-test survey to determine participants' knowledge of privacy after using PARROT. The questions are provided in Appendix A.4.

is measured by counting the number of participants who answered the factual questions both confidently and correctly such as responding with "Definitely yes" if the answer is yes. As seen in Figure 11, the results of the factual questions indicate an increase in accuracy for specific questions, such as Q7, Q9, Q10, and Q11. These questions saw an improvement from 19% to over 50%. Furthermore, the results indicate that PARROT has assisted participants in ensuring proper privacy practices regarding privacy compliance, purpose of use, and general data subject rights as evidenced by the 100% accuracy rate for questions Q1, Q2, and Q4. The confidence-accuracy rate has also shown a significant improvement, with a rise from 6% to 50% for question Q7, and from 0% to 56% and 38% for questions Q2 and Q5, respectively. These results highlight the effectiveness of PARROT in improving general privacy knowledge and understanding among novice developers.

In contrast, the results of the post-test survey on privacy knowledge revealed that PARROT was less effective at questions related to cookies. Specifically, the highest percentage of incorrect answers was observed in questions Q3, Q4, and Q9, which all pertained to cookie banners, with incorrect answers ranging from 31% to 50%, as shown in Figure 12. The same point is illustrated in Figure 13 where 25% of participants were not familiar with purpose assessment and the privacy notice (also known as the cookie banner). This rate decreased to 6% after participants used PARROT for both concepts. Privacy knowledge about the notice was increased after using PARROT with 50% of participants indicating that they had a general understanding and 25% indicating a high level of understanding and ability to implement it. Despite this, most participants were unable to answer the post-test questions related to cookies correctly. This could indicate a lack of clear understanding of the concept of cookies and their privacy-related issues, which can involve complicated technical terms. In Section 6.3, we provide a more detailed discussion of the challenges associated with these features.

6.1.3 How novice developers Perceive PARROT?. In order to evaluate the students' perception of PARROT, we adopted a similar approach as [2, 29, 35], using a 7-point Likert scale to show the level of enjoyment, ease of use, and the likelihood of learning privacy through PARROT. The results

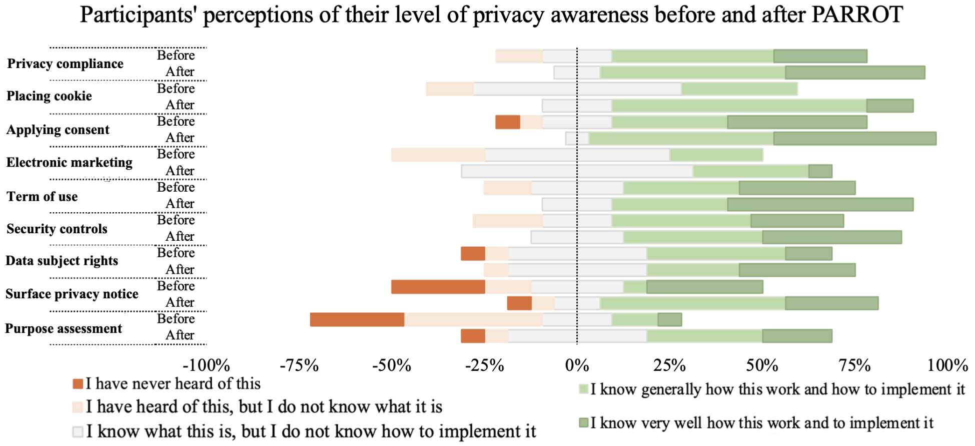


Fig. 13. A comparison of how participants rated their level of privacy awareness about general privacy concepts before and after PARROT.

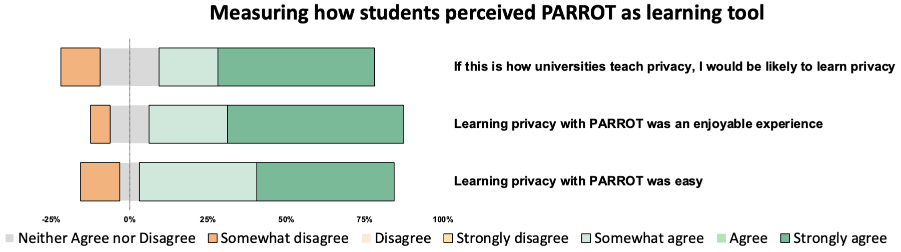


Fig. 14. The perception of PARROT as a privacy-learning tool among novice developers.

indicated that a majority of novice developers found PARROT's features to be engaging and easy to understand due to its interactive nature and the use of colour coding, as seen in Figure 14. Furthermore, the majority expressed positive feedback towards the likelihood of learning privacy through PARROT, with suggestions for enhancing the tool to be an educational tool presented in Section 6.2.4.

6.2 Qualitative Results and Lessons Learned

We also performed a qualitative analysis to have more insight into participants' thoughts and ideas (Studies 1 and 2 participants are referred to as pairs and groups, respectively). Our study followed a qualitative analysis approach using Miles' methods and Richards' coding techniques of descriptive coding, topic coding, and analytical coding [47, 55]. Thematic analysis was used to examine task designs and interviews that were transcribed, coded and analysed for themes [11, 54]. It is our intention to explore how our proposed tool can assist with privacy-aware IoT applications, increase awareness of privacy-preserving laws and measures among software developers, educate novice developers on privacy-preserving legislation and laws, and explore ways to enhance privacy education through co-design with students.

6.2.1 Does PARROT Help Integrate Privacy Principles and Patterns? In Study 1, we investigated the effectiveness of PARROT in integrating privacy principles and patterns through interactions with

Table 4. This table illustrates the familiarity of participants with privacy patterns before and after using PARROT to determine whether the tool helped to make them clearer. The circle's fill reflects the percentage of participants for each choice, based on the number of choices for each option*.

	Without PARROT			With PARROT		
Privacy patterns	Unfamiliar	Somewhat familiar	Familiar	Unfamiliar	Somewhat familiar	Familiar
1. Use of dummies	◕	◔	○	○	◑	◑
2. Location granularity.	◔	◑	◔	○	◔	◕
3. Minimal information asymmetry	◑	◔	◔	◔	◔	◑
4. Asynchronous notice	◑	◔	◔	◔	◔	◕
5. Privacy policy display	◔	◔	◑	○	◔	◕
6. Outsourcing [with consent]	◔	◑	◔	○	◑	◑
7. Onion routing	◑	◔	◔	◔	◑	◔
8. Anonymity set	◑	◔	◔	○	◑	◑
9. Pseudonymous identity	◑	◔	◔	○	◔	◕
10. Privacy icons	◔	◔	◔	◔	◔	◕
11. Data breach notification	◔	◑	◔	◔	◔	◕
12. Privacy dashboard	◑	◔	◔	◔	◑	◑
13. Added-noise obfuscation	◕	◔	◔	◔	◔	◑
14. Increasing aggregation awareness	◕	◔	○	◔	◑	◑
15. Privacy awareness panel	◔	◔	◔	○	◔	◕
16. Obtaining explicit consent	◔	◔	◑	○	◔	◕
17. Informed implicit consent	◔	◔	◔	○	◔	◕
18. Who's listening	◔	◑	◔	○	◔	◕
19. Sticky policies	◑	◔	◔	○	◑	◑
20. Lawful consent	◑	◔	◔	○	◔	◕

* The symbols ◔ ◑ and ◕ represents 25% 50% and 75% of the participants respectively, while ○ represents 0%.

Fig. 15. Themes that emerged from the brainstorming session (last session of Study2:Step 5). Participants' responses to "What does PARROT do in order to support educational learning about privacy? What features should stay, be enhanced or added?"

participants. The participants expressed a preference for PARROT's visual representation, with Pair 2 stating, *"the generated colors are helpful to flag any privacy issue immediately... [we] think it helps* *to rethink the question again"*. Pairs 1, 4 and 5 believed that PARROT could be helpful for individuals without a background in privacy to understand it quickly. Pair 4 stated, *"I definitely struggle to understand and apply privacy and privacy patterns because there are many different documents, laws, and IoT devices. PARROT will tell you already what privacy needs to be fulfilled for that node which is super useful, in my opinion... you don't have to start researching about it."* Additionally, Pairs 1, 4, 5 and 6 reported that the questions posed by PARROT led them to consider new perspectives. Pair 1 stated, *"the questions and visual presentation make me aware of little things... presenting privacy when you are setting up is very helpful."* Pair 4 said that *"the variety of questions you got asked makes you think of how you can make this correctly"* and Pair 5 reported that *"the questions help me to think more about the data subject perspective, not the problem owner only"*. In Study 2, it was observed that PARROT helped to increase the familiarity of novice developers with technical terms related to privacy patterns, as evidenced in Table 3. The results of both Study 1 and Study 2 demonstrate that PARROT's visual representation can effectively integrate privacy principles and be used to familiarise participants with privacy patterns. Additionally, it helps to encourage critical thinking and understanding among participants.

6.2.2 Common Privacy Concerns Among Novice Developers. One key concern among novice developers was the importance of security as a component of privacy. Through observations and discussions, it was found that the majority of groups placed security at the top of their list of priorities. To further underscore the importance of security, almost all groups identified it as their number one priority in regards to their privacy concerns. Initial design decisions frequently included terms such as "*malware*," "*hacker*," and "*encryption*." As the study progressed and participants explored and simulated different designs using PARROT, additional terms such as "*authentication*" and "*access control*" were added to the list of considerations. In addition to security concerns, a common concern that was considered by all participants after simulation of other designs was the server's location.

Moreover, the study identified gaps in knowledge and mindset among participants regarding the collection and storage of data. For example, while some participants agreed that the patient location should not be used in PARROT, they still captured the location. Group 5 argued that the hospital may need to locate the patient even without consent. Group 3 also stated that collecting location is not problematic since the data subject is a patient. This highlights the need for further clarification on PARROT about the importance of obtaining consent from the data subject as per legal requirements. Novice developers should be aware that they do not collect personal data about data subjects because they would like to do so.

The study found that the initial application of privacy patterns by participants was challenging. However, as the study progressed, and participants engaged in additional rounds of exploration and simulation using the PARROT tool, the difficulty of applying certain privacy patterns decreased. This suggests that the PARROT tool can aid in the understanding of privacy patterns, but not to a significant degree. One specific example of this is the consent privacy pattern, where group 4 argued that explicit consent should be obtained, but not implicit consent. These findings highlight the need for further research to investigate the effectiveness of PARROT in supporting the application of privacy patterns.

6.2.3 Clear vs Unclear Features. Does PARROT Appear to Novice Developers to be a Clear and Easy to Learn Educational Tool? The results of the analysis of Figure 15 indicate that the majority of participants (6 out of 7 groups) found that the color coding feature was the most clear and helpful in understanding privacy concepts and configuration. However, Group 7 noted that the node/subnode separation feature was equally helpful to narrow down privacy-specific features. Three groups found the privacy configuration/choices easy to comprehend, and three others found that the quick mapping between the options and the icons made privacy easier to grasp.

With regards to the details of privacy configuration and choices, a mixed reaction was observed. One group commented that the tool provided *"good detail about privacy issues"*, while four others expressed the need for more details such as links to relevant laws, examples of specific privacy issues, and more in-depth explanations, such as a read less/read more option for each choice. Two groups felt that the tool was not clear at first and suggested that a demo option would assist in comprehending its functionality more quickly. Members of Group 1 suggested that the tool could provide additional values to improve privacy clarity. For example, "*for data retention, it [PARROT] asks if you would like to comply with data retention, but it does not specify what the data retention period should be obeying by... for each type of data.*" They also noted that they were not clear regarding risk assessment and recommended presenting an overall score that would update according to their choices. Lastly, two groups noted that the icon font and size were not clear, which can be a problem especially for people with vision issues.

6.2.4 What aspects of learning privacy are addressed, partially addressed, or not addressed by PARROT?. The study examined the effectiveness of PARROT in addressing various aspects of learning privacy. The majority of participants (6 out of 7) reported that the combination of colour coding with immediate mapping and interaction helped them think and learn about privacy, indicating that PARROT fully addresses this aspect of privacy education. Group 1 noted that PARROT prompted them to consider specific details such as ensuring that the server provider is located in the same European Union country as the patient, which the majority of participants agreed should be retained in the design.

However, the study also identified several areas in which PARROT partially addresses learning privacy. These include the need for additional technical configurations for devices, such as specifying the device manufacturer and recommending appropriate data retention based on the application at hand. Additionally, participants suggested using different representations, such as pop-up, tool tip, and slide scale, in addition to the current Yes/No configuration. Participants also noted the need for PARROT to include the law name and number that trigger privacy issues, as well as warnings about missing privacy issues. Furthermore, participants suggested adding an overall score that informs them of their privacy summary and how far they are from fulfilling privacy requirements.

The study also identified areas in which PARROT does not address learning privacy. These include the lack of an import feature for adding new objects that are not predefined. Additionally, Group 6 noted that PARROT is currently designed for individuals with a background in computer science and may not be accessible to users from other backgrounds. *"The tool assumes all users have knowledge of technical details such as encryption,"* Group 5 commented. Furthermore, Group 3 stated that PARROT does not support some technologies such as historical versioning or a prevention icon for threat intelligence. In addition, Group 4 suggested that privacy configuration be presented at multiple levels based on the level of knowledge of the student. In addition, they suggested that the level of notification could be adjusted according to the users' preferences.

The results of the study, as presented in Figure 16, indicate that participants identified a number of potential additions to PARROT that they believe would enhance the learning experience. These features include, but are not limited to, additional technical configurations, improved representation options, and the inclusion of specific laws and warnings. These findings suggest that there may be opportunities to further improve the effectiveness of PARROT as a tool for educating individuals about privacy.

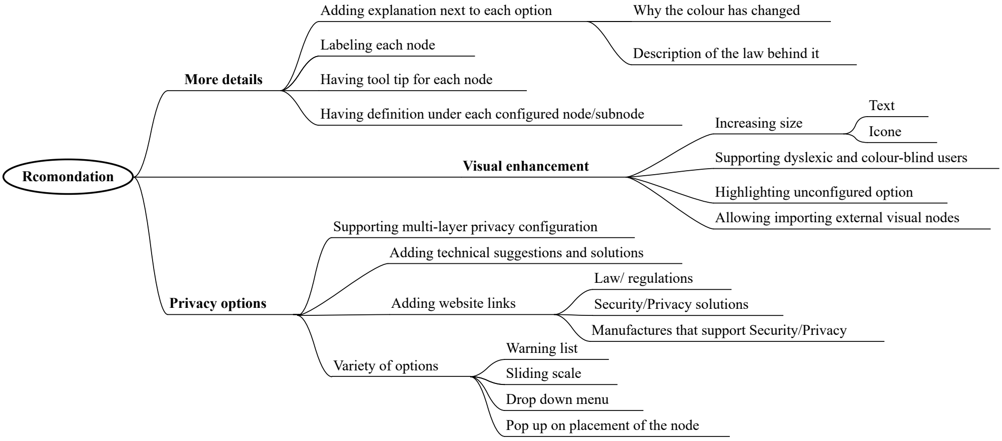

Rcomondation
More details
Adding explanation next to each option
Why the colour has changed
Description of the law behind it
Labeling each node
Having tool tip for each node
Having definition under each configured node/subnode
Visual enhancement
Increasing size
Text
Icone
Supporting dyslexic and colour-blind users
Highlighting unconfigured option
Allowing importing external visual nodes
Privacy options
Supporting multi-layer privacy configuration
Adding technical suggestions and solutions
Adding website links
Law/ regulations
Security/Privacy solutions
Manufactures that support Security/Privacy
Variety of options
Warning list
Sliding scale
Drop down menu
Pop up on placement of the node

Fig. 16. A taxonomy of enhancement suggestions made by participants to support privacy education.

6.3 Challenges and future work

In the context of the CGM scenario, it appears that there is a challenge in distinguishing the app's primary purpose of collecting glucose readings from its potential to collect GPS data in the event of an adverse incident. The idea of adding GPS location data collection to the feature may arise among participants, which is not entirely unreasonable given the legal requirement that cars transmit GPS location information in the event of a collision (i.e. eCall [22]). There are, however, strict limitations to this procedure, since it is only activated by an impact. This may suggest that PARROT may also include a feature that can protect user privacy in a manner similar to the car scenario. Possibly, this could involve transmitting GPS data to emergency services in a controlled manner, which could enhance the tool and provide valuable public service.

Looking at the novice developers' responses to factual and post-test privacy questions, it shows that the novice developers' lack of clarity regarding the cookie and purpose of assessments which was expected and noted by the lawyer, who stated that "it is a grey area" and that while developers at startups may need to address the matter, larger organizations may delegate this responsibility to somebody else. However, "they should know that the fail safe position is to always develop functionality that can surface a cookie banner and capture separate consent for different categories of cookies" the lawyer continued. The tool should be able to handle that requirement for assisting developers. Both the privacy notice and the purpose of assessments should be incorporated into the student's education, according to the lawyer.

There are so many challenges with third party cookies, which are most often used for advertising and targeting. This is because the website/app owner will need to capture consent for the placement of these cookies and ensure that they are accurately described in the cookie notice. Making this simple to understand in a design tool is challenging. There is therefore a need for further investigation and improvement in PARROT's ability to educate users on cookie-related privacy issues and the importance of purpose assessment. However, it has been reported that despite receiving technical and legal information, individuals do not increase their motivation to reject tracking cookies [64]. It is possible that this is due to the fact that cookies are often regarded as harmless since they are used to store preferences and enhance the user's experience. "What novice developers don't realise is what's going on behind the scenes" the lawyer explained. Many people assume that they are familiar with cookies without fully comprehending the potential for online tracking, including the monitoring of websites visited, purchases made, and search queries ...etc.

7 CONCLUSION

In this paper, the PARROT tool is used to demonstrate the importance of incorporating privacy into the design of IoT applications. Our research shows collaboration with privacy professionals and a privacy lawyer, which led to the identification of privacy risks in less-regulated domains. We discuss the findings of our PARROT two lab studies. These results indicate the effectiveness of the PARROT prototype tool in promoting privacy awareness and understanding during the design of IoT applications. Participants who used PARROT had a better understanding of how personal data is handled and were able to design more privacy-aware IoT solutions. Co-designing with novice developers provided insights into potential enhancements to the PARROT prototype tool as a privacy education tool. Collaboration allowed for a thorough exploration of the tool's capabilities and limitations and the potential for improvement as an educational tool. Even though PARROT does not guarantee that IoT systems built using it will be free of all privacy issues, we believe software developers will have a better understanding of privacy principles.

REFERENCES

[1] Atif Ahmad, Sean B. Maynard, Kevin C. Desouza, James Kotsias, Monica T. Whitty, and Richard L. Baskerville. 2021. How can organizations develop situation awareness for incident response: A case study of management practice. *Computers and Security* 101 (2021), 102122.

[2] Nada Alhirabi, Stephanie Beaumont, Jose Tomas Llanos, Dulani Meedeniya, Omer Rana, and Charith Perera. 2023. PARROT : Interactive Privacy-Aware Internet of Things Application Design Tool. *Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies* 7, 1 (2023).

[3] Nada Alhirabi, Omer Rana, and Charith Perera. 2021. Security and Privacy Requirements for the Internet of Things: A Survey. *ACM Trans. Internet Things* 2, 1, Article 6 (Feb 2021), 37 pages.

[4] Nada Alhirabi, Omer Rana, and Charith Perera. 2022. Demo Abstract: PARROT: Privacy by Design Tool for Internet of Things. In *2022 IEEE/ACM Seventh International Conference on Internet-of-Things Design and Implementation (IoTDI)*. 107–108.

[5] Apple. 2022. User Privacy and Data Use.

[6] Vanessa Ayala-Rivera and Liliana Pasquale. 2018. The grace period has ended: An approach to operationalize GDPR requirements. In *2018 IEEE 26th International Requirements Engineering Conference (RE)*. IEEE, 136–146.

[7] Rebecca Balebako, Jaeyeon Jung, Wei Lu, Lorrie Faith Cranor, and Carolyn Nguyen. 2013. Little brothers watching you:" raising awareness of data leaks on smartphones. *SOUPS 2013 - Proceedings of the 9th Symposium on Usable Privacy and Security* (2013).

[8] Masoud Barati, Gagangeet Singh Aujla, Jose Tomas Llanos, Kwabena Adu Duodu, Omer F Rana, Madeline Carr, and Rajiv Rajan. 2021. Privacy-Aware cloud auditing for gdpr compliance verification in online healthcare. *IEEE Transactions on Industrial Informatics* (2021).

[9] Muhammad Bilal, Abdullah Gani, Muhammad Ikram Ullah Lali, Mohsen Marjani, and Nadia Malik. 2019. Social profiling: A review, taxonomy, and challenges. *Cyberpsychology, Behavior, and Social Networking* 22, 7 (2019), 433–450.

[10] Joshua A. Braun and Jessica L. Eklund. 2019. Fake News, Real Money: Ad Tech Platforms, Profit-Driven Hoaxes, and the Business of Journalism. *Digital Journalism* 7, 1 (2019), 1–21.

[11] Virginia Braun and Victoria Clarke. 2006. Using thematic analysis in psychology. *Qualitative research in psychology* 3, 2 (2006), 77–101.

[12] Lee A Bygrave. 2017. Data protection by design and by default: deciphering the EU's legislative requirements. *Oslo Law Review* 4, 2 (2017), 105–120.

[13] Ann Cavoukian. 2009. Privacy by design: The 7 foundational principles. *Information and privacy commissioner of Ontario, Canada* 5 (2009), 12.

[14] Eric S. Chung, Jason I. Hong, Lin James, Madhu K. Prabaker, James A. Landay, and Alan L. Liu. 2004. Development and evaluation of emerging design patterns for ubiquitous computing. *DIS2004 - Designing Interactive Systems: Across the Spectrum* (2004), 233–242.

[15] Sunny Consolvo, Jaeyeon Jung, Ben Greenstein, Pauline Powledge, Gabriel Maganis, and Daniel Avrahami. 2010. The Wi-Fi privacy ticker: Improving awareness & control of personal information exposure on Wi-Fi. *UbiComp'10 - Proceedings of the 2010 ACM Conference on Ubiquitous Computing* (2010), 321–330.

[16] Lorrie Faith Cranor, Praveen Guduru, and Manjula Arjula. 2006. User interfaces for privacy agents. *ACM Transactions on Computer-Human Interaction (TOCHI)* 13, 2 (2006), 135–178.

[17] Mina Deng, Kim Wuyts, Riccardo Scandariato, Bart Preneel, and Wouter Joosen. 2011. A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements. *Requirements Engineering* 16, 1 (2011), 3–32.

[18] Vasiliki Diamantopoulou, Christos Kalloniatis, Stefanos Gritzalis, and Haralambos Mouratidis. 2017. Supporting privacy by design using privacy process patterns. In *IFIP International Conference on ICT Systems Security and Privacy Protection*. Springer, 491–505.

[19] Vasiliki Diamantopoulou, Christos Kalloniatis, Stefanos Gritzalis, and Haralambos Mouratidis. 2017. Supporting privacy by design using privacy process patterns. *IFIP Advances in Information and Communication Technology* 502 (2017), 491–505.

[20] Nick Doty and Mohit Gupta. 2013. Privacy design patterns and anti-patterns patterns misapplied and unintended consequences. (2013).

[21] Edward S Dove and Jiahong Chen. 2020. To What Extent Does the EU General Data Protection Regulation (GDPR) Apply to Citizen Scientist-Led Health Research with Mobile Devices? *The Journal of Law, Medicine & Ethics* 48, 1_suppl (2020), 187–195.

[22] EDPB. 2020. Guidelines 1/2020 on processing personal data in the context of connected vehicles and mobility related applications.

[23] Dorothy Forbes. 2013. Blinding: An essential component in decreasing risk of bias in experimental designs. *Evidence-Based Nursing* 16, 3 (2013), 70–71.

[24] Damien Geradin, Theano Karanikioti, and Dimitrios Katsifis. 2021. *GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech*. Vol. 17. Taylor & Francis. 47–92 pages.

[25] Nina Gerber, Paul Gerber, Hannah Drews, Elisa Kirchner, Noah Schlegel, Tim Schmidt, and Lena Scholz. 2018. FoxIT: Enhancing mobile users' privacy behavior by increasing knowledge and awareness. *ACM International Conference Proceeding Series* (2018).

[26] Google. 2022. Advertising ID.

[27] Cornelia Graf, Peter Wolkerstorfer, Arjan Geven, and Manfred Tscheligi. 2010. A Pattern Collection for Privacy Enhancing Technology. *The Second International Conferences of Pervasive Patterns and Applications (Patterns 2010)* 2, 1 (2010), 72–77.

[28] Wentao Guo, Jay Rodolitz, and Eleanor Birrell. 2020. Poli-see: An Interactive Tool for Visualizing Privacy Policies. , 57–71 pages.

[29] Wentao Guo, Jay Rodolitz, and Eleanor Birrell. 2020. Poli-see: An Interactive Tool for Visualizing Privacy Policies. *WPES 2020 - Proceedings of the 19th Workshop on Privacy in the Electronic Society* (2020), 57–71.

[30] Martin Höst, Björn Regnell, and Claes Wohlin. 2000. Using students as subjects—a comparative study of students and professionals in lead-time impact assessment. *Empirical Software Engineering* 5, 3 (2000), 201–214.

[31] Michael Howard and Steve Lipner. 2006. *The security development lifecycle*. Vol. 8. Microsoft Press Redmond.

[32] ICO. 2021. ICO calls on Google and other companies to eliminate existing privacy risks posed by adtech industry.

[33] Information Commissioner's Office. 2014. Data controllers and data processors: what the difference is and what the governance implications are. (2014), 20.

[34] Harris Interactive. 2001. Privacy Leadership Initiative: Privacy Notices Research Final Results, Dec. 2001.

[35] Ruogu Kang, Laura Dabbish, Nathaniel Fruchter, and Sara Kiesler. 2019. "My data just goes everywhere:" User mental models of the internet and implications for privacy and security. *SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security* (2019), 39–52.

[36] Sumitkumar Kanoje, Debajyoti Mukhopadhyay, and Sheetal Girase. 2016. User Profiling for University Recommender System Using Automatic Information Retrieval. *Physics Procedia* 78, December 2015 (2016), 5–12.

[37] Barbara A Kitchenham and Tore Dybå. 2004. Evidence-based Software Engineering. (2004).

[38] Sachin Kumar, Prayag Tiwari, and Mikhail Zymbler. 2019. Internet of Things is a revolutionary approach for future technology enhancement: a review. *Journal of Big Data* 6, 1 (2019).

[39] Germán Leiva and et al. 2019. Enact: Reducing designer–developer breakdowns when prototyping custom interactions. *ACM Transactions on Computer-Human Interaction (TOCHI)* 26, 3 (2019), 1–48.

[40] Jorg Lenhard, Lothar Fritsch, and Sebastian Herold. 2017. A literature study on privacy patterns research. *Proceedings - 43rd Euromicro Conference on Software Engineering and Advanced Applications, SEAA 2017* (2017), 194–201.

[41] Tianshi Li, Yuvraj Agarwal, and Jason I. Hong. 2018. Coconut: An IDE Plugin for Developing Privacy-Friendly Apps. *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.* 2, 4, Article 178 (Dec 2018), 35 pages.

[42] Tianshi Li, Elizabeth Louie, Laura Dabbish, and Jason I. Hong. 2021. How Developers Talk About Personal Data and What It Means for User Privacy. *Proceedings of the ACM on Human-Computer Interaction* 4, CSCW3 (2021), 1–28.

[43] Jialiu Lin, Shahriyar Amini, Jason I. Hong, Norman Sadeh, Janne Lindqvist, and Joy Zhang. 2012. Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. *UbiComp'12 - Proceedings of the 2012 ACM Conference on Ubiquitous Computing* (2012), 501–510.

[44] Delfina Malandrino, Vittorio Scarano, and Raffaele Spinelli. 2013. How increased awareness can impact attitudes and behaviors toward online privacy protection. *Proceedings - SocialCom/PASSAT/BigData/EconCom/BioMedCom 2013* (2013), 57–62.

[45] Meta. 2022. About Connections Targeting.

[46] Meta. 2023. About Targeting and Reporting for Automated App Ads. Accessed 16-1-2023.

[47] Matthew B Miles, A Michael Huberman, and Johnny Saldaña. 2018. *Qualitative data analysis: A methods sourcebook.* Sage publications.

[48] Chulhong Min, Seungchul Lee, Changhun Lee, Youngki Lee, Seungwoo Kang, Seungpyo Choi, Wonjung Kim, and Junehwa Song. 2016. PADA: Power-aware development assistant for mobile sensing applications. *UbiComp 2016 - Proceedings of the 2016 ACM International Joint Conference on Pervasive and Ubiquitous Computing* (2016), 946–957.

[49] Sebastian Pape and Kai Rannenberg. 2019. Applying Privacy Patterns to the Internet of Things' (IoT) Architecture. *Mobile Networks and Applications* 24, 3 (2019), 925–933.

[50] Charith Perera, Mahmoud Barhamgi, Arosha K Bandara, Muhammad Ajmal, Blaine Price, and Bashar Nuseibeh. 2020. Designing privacy-aware internet of things applications. *Information Sciences* 512 (2020), 238–257.

[51] Charith Perera, Mahmoud Barhamgi, and Massimo Vecchio. 2021. Envisioning Tool Support for Designing Privacy-Aware Internet of Thing Applications. *IEEE Internet of Things Magazine* 4, 1 (2021), 78–83.

[52] Georgios Petkos, Symeon Papadopoulos, and Yiannis Kompatsiaris. 2015. PScore: A framework for enhancing privacy awareness in online social networks. *Proceedings - 10th International Conference on Availability, Reliability and Security, ARES 2015* (2015), 592–600.

[53] Stefanie Pötzsch. 2008. Privacy awareness: A means to solve the privacy paradox?. In *IFIP Summer School on the Future of Identity in the Information Society.* Springer, 226–236.

[54] Keith F Punch. 2013. *Introduction to social research: Quantitative and qualitative approaches.* Sage publications.

[55] Lyn Richards. 2020. *Handling qualitative data: A practical guide.* Sage publications.

[56] Sasha Romanosky, Alessandro Acquisti, Jason Hong, Lorrie Faith Cranor, and Batya Friedman. 2006. Privacy patterns for online interactions. In *Proceedings of the 2006 conference on Pattern languages of programs.* 1–9.

[57] Paula T. Ross and Nikki L. Bibler Zaidi. 2019. Limited by our limitations. *Perspectives on Medical Education* 8, 4 (2019), 261–264.

[58] A Sadeghi, C Wachsmann, and M Waidner. 2015. Security and privacy challenges in industrial Internet of Things. In *2015 52nd ACM/EDAC/IEEE Design Automation Conference (DAC).* 1–6.

[59] Miraqa Safi, Sajjad Dadkhah, Farzaneh Shoeleh, Hassan Mahdikhani, Heather Molyneaux, and Ali A. Ghorbani. 2022. A Survey on IoT Profiling, Fingerprinting, and Identification. *ACM Trans. Internet Things* 3, 4, Article 26 (sep 2022), 39 pages. https://doi.org/10.1145/3539736

[60] Merve Sahin, Tolga Unlu, Cedric Hebert, Lynsay A. Shepherd, Natalie Coull, and Colin Mc Lean. 2022. Measuring Developers' Web Security Awareness from Attack and Defense Perspectives. *Proceedings - 43rd IEEE Symposium on Security and Privacy Workshops, SPW 2022* (2022), 31–43.

[61] Till Schümmer. 2004. The public privacy–patterns for filtering personal information in collaborative systems. In *Proceedings of CHI workshop on Human-Computer-Human-Interaction Patterns.* 1–35.

[62] Robert W Shirey. 2007. Internet Security Glossary, Version 2. RFC 4949.

[63] Forrest Shull, Janice Singer, and Dag I.K. Sjøberg. 2008. *Guide to advanced empirical software engineering.* 1–388 pages.

[64] Joanna Strycharz, Edith Smit, Natali Helberger, and Guda van Noort. 2021. No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior* 120 (2021), 106750.

[65] Mohammad Tahaei, Alisa Frik, and Kami Vaniea. 2021. Privacy champions in sofware teams: Understanding their motivations, strategies, and challenges. *Conference on Human Factors in Computing Systems - Proceedings* (2021).

[66] Michael Veale and Frederik Zuiderveen Borgesius. 2021. Adtech and Real-Time Bidding under European Data Protection Law. (2021), 1–37.

[67] Wirewheel. 2021. Data Privacy Laws in 2021: What You Need to Know.

[68] Robert K Yin. 2018. *Case study research and applications.* Sage.

[69] Joseph W. J.W. Yoder and Jeffrey Barcalow. 1998. Architectural patterns for enabling application security. *Proceedings of PLoP 1997* 51 (1998), 31.

[70] Shuai Yuan, Jun Wang, and Xiaoxue Zhao. 2013. Real-time bidding for online advertising. (2013), 1–8.

A INTERVIEWS QUESTIONS

A.1 General Background Questions

- Email Address:
- Participant ID (your first name . e.g. Nada) [Study use only]
- Age group:[20-29][30-39][40-49][50-59][60+]
- Qualification:
  - Diploma
  - Bachelor's degree (or equivalent)
  - Master's degree (or equivalent)
  - Doctoral Degree (or equivalent)
- How many years of experience do you have in SW development?
- What is your area of expertise?

A.2 Factual/knowledge Questions

As a developer answer based on what you did on your privacy design decision sheet and your pre-existing knowledge. The answers were rated on a 5-point Likret scale: "Definitely no," "Probably no," "Unsure," "Probable yes," and "Definitely yes." *Correct answer means the best privacy practice that developer need to know. **Participants are also asked to answer the same questions after using PARROT.

	Question	Correct answer*
Q1	I know that privacy compliance is needed for all types of personal data.	Yes
Q2	Did you clearly decide what features the app should have and what Personal Data (PD) you might need to collect prior to the development process?	Yes
Q3	If you use PD in your app: Do you clearly know the purpose for that?	Yes
Q4	Do you think your app users should clearly know about what Personal Data (PD) are used and how they are used?	Yes
Q5	Did you know what data app users should be able to (delete, correct, and download a copy of their data) and how?	Yes
Q6	Did you store personal identifiable information (PII) /Personal Data (PD) safely?	Yes
Q7	Did you specify the duration for storing Personal Data (PD)?	Yes
Q8	It is acceptable to store or process user data for long duration for another purposes such as analytics.	-
Q9	Do you know if PII or PD will be shared by what apps?	Yes
Q10	Do you know the best privacy practices with analytical/ advertising third-party libraries?	Yes
Q11	Are you familiar with the data collection practices of the libraries that you used?	Yes

A.3 General Privacy Self Report Scale

How would you rate your level of privacy awareness and frequency of use of the following concepts (general concepts): *Participants are also asked to answer the same questions after using PARROT. **Some of the questions are inspired by [35] paper.
1. Privacy compliance: (A) - (B) - (C) - (D) - (E)
2. Placing cookie: (A) - (B) - (C) - (D) - (E)
3. Applying consent: (A) - (B) - (C) - (D) - (E)
4. Electronic marketing: (A) - (B) - (C) - (D) - (E)
5. Term of use: (A) - (B) - (C) - (D) - (E)
6. Security controls: (A) - (B) - (C) - (D) - (E)

Choice code	Explanation
A	I have never heard of this
B	I have heard of this, but I do not know what it is
C	I know what this is, but I do not know how to implement it
D	I know generally how this work and how to implement it
E	I know very well how this work and to implement it

7. Data subject rights: (A) - (B) - (C) - (D) - (E)
8. Surface privacy notice: (A) - (B) - (C) - (D) - (E)
9. Purpose assessment: (A) - (B) - (C) - (D) - (E)

A.4 Post-test Knowledge Survey

Could you please indicate whether each of the following statements is true or false? If you are unsure of the answer, select "Not sure".

	Question Text	True	False	Not sure
Q1.	*Does an organisation always need data subjects' consent for all sensitive personal data?*	X		
Q2.	*Parental authorization is only needed if an individual is under 10 (in GDPR).*		X	
Q3.	*The cookie banner must be surfaced once despite browser settings changed.*		X	
Q4.	*Analytics and Ad/targeting cookies need to place surface cookies banner only.*		X	
Q5.	*We need to capture consent to the type of marketing when electronic marketing is used.*	X		
Q6.	*Processing data that are not needed for the purpose is acceptable.*		X	
Q7.	*No need for privacy compliance if there is no sensitive personal data.*		X	
Q8.	*We need to capture the "agree to term of use" from the user once, despite browser settings change.*	X		
Q9.	*We need to use surface cookie banner only if only necessary cookies are used.*	X		
Q10.	*If analytics cookies or Ad/targeting cookies are used, we need to use a surface cookies banner, capture consent or acceptance, and place cookies according to consent.*	X		
Q11.	*Data subject rights are for - access – deletion - data portability.*	X		
Q12.	*If third parties are involved security assessment is not needed.*		X	

B PARROT MAPPING

Table 5. Sample of applying privacy patterns to help developers develop privacy aware IoT applications. We chose privacy patterns that applicable to the selected use cases and may help developers think about privacy throughout the design lifecycle.

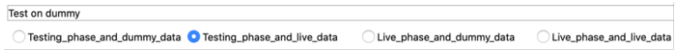
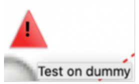
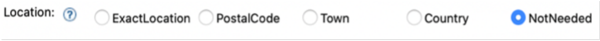
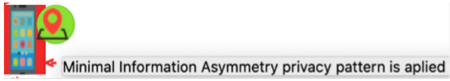
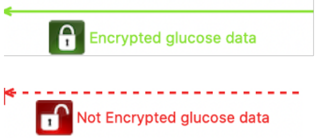
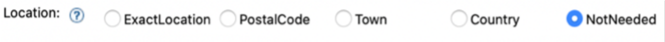
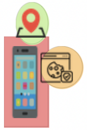
Privacy pattern list	Example	Visual representation
Use of dummies	The tool offers the possibility to test the dummy or real data in the testing or live phase. This will give a warning to the developer so they can know what will happen in the testing phase.	**The displayed choices:**  Test on dummy ○ Testing_phase_and_dummy_data ● Testing_phase_and_live_data ○ Live_phase_and_dummy_data ○ Live_phase_and_live_data **The displayed effect of the choice:**  Test on dummy
Location Granularity	The developer should give the user (patient) options on the granularity of their location data that may be shared.	 Location: ? ○ ExactLocation ○ PostalCode ○ Town ○ Country ● NotNeeded
Minimal Information Asymmetry	The developer needs to ensure that the system collects only necessary data. For example, when the patient's location checkbox is ticked with the 'not needed' choice, the message that applies the Minimal Information Asymmetry idea will be shown when hovering over the location icon.	 Minimal Information Asymmetry privacy pattern is aplied
Asynchronous Notice	Each time patient data is being sent, a noticeable change should be shown to the developer. This will help the developer apply the same action to the user. For example, when sending glucose data from the sensor to the phone, the colour of the sent data will change depending on whether it is encrypted.	 Encrypted glucose data Not Encrypted glucose data
Privacy Policy Display	The tool should allow developers to see the privacy policy from the beginning. For example, the colour of the icon is displayed and changed based on the choices of Location Granularity privacy patterns.	**The displayed choices:**  Location: ? ○ ExactLocation ○ PostalCode ○ Town ○ Country ● NotNeeded **The displayed effect of the choice:** 

Table 6. The table below lists 20 privacy patterns that were applied to the online pharmacy use-case. Sources: (privacypatterns.org) and (privacypatterns.eu).

	Privacy patterns	Explanation	GDPR Article	Applicable node
1.	Use of dummies	The dummies are used for personal data, so the system should vague the data subject's data by adding fake data to the database.	A. 32: Security of processing.	All clouds
2.	Location granularity	The data subject should have the choice to share the level of location details.	A. 5: Purpose limitation & Data Minimisation.	Website & mobile app
3.	Minimal information asymmetry	Data collected, and privacy policies should be clearly known to the data subject as much as the controller knows.	A. 5(and Recital 39): lawfulness, fairness and transparency & Data Minimisation.	Website & mobile app
4.	Asynchronous notice	Each time data subject data is being sent a notification should be given to the data subject.	A. 13 – 14: Information to be provided where personal data are collected/ not obtained.	Website & mobile app
5.	Privacy policy display	The system should display the privacy policy at the beginning.	A. 5 (and Recital 39): lawfulness, fairness and transparency.	Website & mobile app
6.	Outsourcing [with consent]	The controller should obtain additional law consent from data subjects before processing their data to third parties such as sharing with shipment companies.	A. 6: Lawfulness of Processing.	Data subject
7.	Onion routing	Transferred data should be encrypted in layers, each edge decrypts a layer.	A. 5: Integrity and confidentiality. A. 33: Notification of a personal data breach. A. 32: Security of processing.	Over all the links
8.	Anonymity set	The system should apply anonymity set mechanism that anonymous data subject identity by limiting the positions where data subjects can be located.	A. 32: Security of processing.	All the clouds (on data sharing)
9.	Pseudonymous identity	From social company perspective, it does not need to know the data subject identity, the social company should only have access to the location and other impersonal data, such as, IP address.	A. 32: Security of processing.	Links: Pharmacy cloud host cloud, Host cloud social cloud & real bidding cloud
10.	Privacy icons	The privacy polices document should afford standardized visual icon sets beside text which will help data subjects to understand the policies easier.	A.5 (and Recital 39): Lawfulness, fairness and transparency.	Website & mobile app
11.	Data breach notification pattern	The application should react to a data breach quickly by notifying the data subject with the breach details.	A.5: Integrity and confidentiality. A.9.1 : Processing of special categories of personal data. A. 24 -: Accountability. A.33: Notification of a personal data breach. A.37: Designation of the data protection officer.	All the clouds (controller and processors) & Website & mobile app
12.	Privacy dashboard	The data subject should be able to view all his collected data easily in summarized design at the application interface.	A. 7: Conditions for consent. A. 13 – 14: Information to be provided where personal data are collected/ not obtained. A. 15: Right of access by the data subject. A. 16: Right to rectification. A. 17: Right to erasure ('right to be forgotten'). A. 18: Right to restriction of processing. A. 21: Right to object. A. 22: Automated individual decision-making, including profiling.	Website & mobile app

13.	Added-noise obfuscation	Add false values to the data subject's records that would be cancelled automatically in a long term.	A. 5: Purpose limitation.	All clouds
14.	Increasing aggregation awareness	The system should inform and apply aggregation as much as possible.	A. 5(and Recital 39): lawfulness, fairness and transparency.	Website & mobile app (similar to privacy dashboard)
15.	Privacy awareness panel	In the application, the data subject should be clearly aware that his data are sent to third parties such as shipment company.	A. 5 (and Recital 39): lawfulness, fairness and transparency.	Website & mobile app
16.	Obtaining explicit consent	The data subject should be given explicit consent via the application that sufficiently explains the consequences of providing their data.	A. 6: Lawfulness of Processing. A. 7 (and Recital 11): Conditions for consent. A. 8: Conditions applicable to child's consent.	Data subject
17.	Informed implicit consent	The data subject should be sufficiently informed of all data that are collected about him via the application.	A. 5 (and Recital 39): Lawfulness, fairness and transparency. A. 7: (and Recital 11): Conditions for consent. A. 8: Conditions applicable to child's consent.	Website & mobile app
18.	Who's listening	Data subject should be able to know who have the access to view his data. For example, the data subject should know that the social and shipment companies have accessed the location data.	A. 13 – 14: Information to be provided where personal data are collected/ not obtained.	Website & mobile app
19.	Sticky policies	The system should stick to the policies although it shares data with third parties.	A. 5: Data Minimisation. A. 5: Storage limitation. A. 24 : Accountability. A. 37: Designation of the data protection officer.	All clouds (on data sharing)
20.	Lawful consent	The data subject should provide a consent if he wants to share his data with others such as social company.	A. 5: Purpose Limitation. A. 6: Lawfulness of Processing. A. 7: (and Recital 11): Conditions for consent. A. 8: Conditions applicable to child's consent.	Data subject