Demo Abstract: PARROT: Privacy by Design Tool for Internet of Things

Nada Alhirabi
School of Computer Science and Informatics, Cardiff University
Cardiff, UK
King Saud University, Saudi Arabia
AlhirabiN@cardiff.ac.uk

Omer Rana
School of Computer Science and Informatics, Cardiff University
Cardiff, UK
RanaOF@cardiff.ac.uk

Charith Perera
School of Computer Science and Informatics, Cardiff University
Cardiff, UK
PereraC@cardiff.ac.uk

***Abstract*—The design process for applications that make use of Internet of Things (IoT) can be more complex than for desktop, mobile or web-based platforms. IoT applications typically collect and analyse personal data categorised as *sensitive*. These data may be subject to a higher degree of protection under data privacy laws. We present PARROT (PrivAcy by design tool foR inteRnet Of Things) – an interactive IoT application design tool for privacy-aware IoT applications. PARROT enables developers to consider privacy compliance during the design process and provides real-time feedback on potential privacy concerns that may need to be considered. From a privacy compliance perspective, PARROT incorporates privacy-specific design features into the IoT application from the beginning rather than retrospectively.**

***Index Terms*—Internet of Things, Privacy by Design, Software Design, Data Protection, Privacy Law, GDPR, Usable Privacy**

I. INTRODUCTION AND MOTIVATION

Internet of Things (IoT) applications generate and process large amounts of data, which need to be transferred to devices for processing. As the size and frequency of generation of this data increases, an efficient architecture is needed to deal with this data. To enable end-users to use these applications regularly, it is necessary to design End-User Development (EUD) techniques that align more closely with user needs. Interactivity may also make such applications and software tools more intuitive for users (both lawyers and developers in our case). It is necessary for EUD techniques to more closely capture real-time collaboration instead of a static user experience.

Researchers have been using privacy-enhancing technologies (PETs) and privacy-by-design (PbD) concepts to minimise privacy risks in data processing systems. These approaches must align with legal privacy requirements, such as those set out in the General Data Protection Regulation (GDPR). Data protection-by-design (DPbD) must ensure that privacy-related requirements are considered in the design and development of data processing systems [1]. Cavoukian [2] identified the importance of including PbD into the design of information technologies and systems. Despite the efforts made in the PbD area, most people have limited knowledge of (potentially substantial) privacy risks in an online environment. Many users find it difficult and time-consuming to fully understand privacy policies and their impact on their work. There is a need for a tool that enable privacy requirements to be more clearly identified [3] [4] [5]. This tool should also offer an intuitive and user-friendly interfaces to assist software developers in deciding how to include privacy into their system design.

II. APPROACH

We used a number of semi-structured interviews to understand privacy requirements of users, including collaboration with a privacy lawyer. This led to the design and implementation of PARROT. A prototype of PARROT was then evaluated to see if developers considered privacy requirements during the design process.

A. Study 1: Understanding Privacy Breakdowns

The goal of this study was to understand privacy challenges considered by developers. To design our tool we recruited 18 full-stack developers to examine their understanding of privacy through a series of semi-structured interviews. We then ran an IoT application design exercise for an IoT health use case, *Diabetes treatment and monitoring*, to understand their approach of integrating privacy within the software design process. We collaborated with a privacy lawyer and other legal professionals to identify privacy breakdowns between developers and privacy professionals. Our results helped us to identify potential areas to consider for the design of IoT applications.

B. Study 2: Operationalisation

This study aimed to apply operationalisation techniques for the designs produced in study one. We applied the design notations that were analysed in study one using the four Enact design principles: provide multiple viewpoints, maintain a single source of truth, reveal the invisible, support design by enaction [6]. Since Enact principles claimed to reduce the breakdown between designers and developers, we wanted to test whether the same principles could help us to reduce breakdowns between developers and privacy professional.