Privacy’s 7Cs and the Crowded Augmented Reality User: A Position Paper

Dawn N. Jutla\textsuperscript{1} and Peter Bodorik\textsuperscript{2}
\textsuperscript{1}Sobey School of Business, Saint Mary’s University
\textsuperscript{2}Faculty of Computer Science, Dalhousie University, Halifax, NS, Canada

Introduction

Consider scaling user privacy in augmented reality (AR) and Internet of Things (IoT) environments where many users own AR apps on phones, watches, bracelets, neck ornaments, eyeglasses, and cars, and communicating devices are also in IoT surroundings. An approving user, who consents to the use of her image with a smiling nod, is imaginable. She provides permission when she has time to communicate. When her time is limited, or the requests to use her personal data are too numerous, she may entrust her mobile machine agents to automatically share her privacy preferences with requesting devices.

This crowded, busy user scenario (Fig. 1) leads to the following software engineering and business issues and questions, among others, in the AR and IoT environments:

(1) The functionality to preserve the 7Cs privacy properties (comprehension (e.g. via notice), consciousness, choice, consent, consistency, consistency, and context [3]) that we ideally need on the user side is not all commercially available. Personal privacy agents, or equivalent, are needed to implement a whole array of automatic/automated user privacy services (e.g. notice, agreement, preference sharing, validation, de-identification, pseudonymization etc.), and to communicate with other machines. Software engineers will likely build clever lightweight machine “agents” and “services” to automate users’ permissions, preferences, and record automated notices in the AR and IoT environments, using a plethora of techniques (e.g. as in [3] and [4]).

(2) The user will generate Big Data every day with constant communication with AR-enabled, mobile apps, and/or Internet of Things’ devices. Where will the power relationships lie in business models? The user will be the primary and most reliable aggregator of her daily Big Data, but conversely fragmentation protects privacy. Where will she store her data, and who will own it? Will she be able to realistically afford storage fees for her burgeoning personal cloud? If not, what will be the business model(s) that software engineers will enable for the user, the data storage provider, the AR platform owners/providers, the mobile device operators, and can this list of non-user stakeholders respect the user’s privacy, or will they incent her privacy away from her? Indeed, how can the user empower...
himself to take control over his privacy when most organizations prefer to keep control of users’ data, and may not “play ball”? Are the fundamental concepts of control over one’s information, as embedded in the vendor relationship management (VRM) movement, enough to disrupt the mass market? Will marquee firms across every industry decide to compete on protecting user privacy, and will they create new and attractive privacy-respecting business models for users that other organizations would be required to imitate? The VRM-based Respect Network [9] currently shows IT and telecommunication industry players as beachheads. But we need privacy to be respected by the mainstream. If the vision and passion for creating privacy-respecting software fans out further, technologists may yet create a sustainable future with socially-responsible software platforms.

(3) With such a privacy-protecting future in mind, and to scale gracefully while refraining from overloading the user, AR systems will need to communicate with users’ privacy/preference agents in a standardized way. Approved industry standard(s) for their interface is/are not yet built. However, progress towards privacy standards is evident in this second decade of the 21st century. The OASIS Privacy Management Reference Model and Methodology (PMRM) and OASIS Privacy by Design Documentation for Software Engineers (PbD-SE) are examples of recent and promising standard-track work products. There is new user demand for the Platform for Privacy Preferences (P3P) [7] and these OASIS emerging standards in the AR, IoT, and Big Data environments. If industry accepts their social responsibilities to future societies, software engineers may need to know these and other pertinent standard(s) to embed privacy requirements and functionality in their AR systems. How can we take privacy engineering to the mainstream? What are we doing as a collective to get institutional stakeholders to buy in?

Privacy Notices: Complicated by Layering of Platforms

Getting stakeholders to have interoperable and consistent privacy policies within the same organization is a challenge [1]. Across platforms, owned by different organizations, the problem exacerbates greatly. P3P, the Platform for Privacy Preferences [8], provides for automatic reading of privacy notices and matching to user privacy preferences, but P3P has not yet been robustly applied in the
situation as depicted in Fig. 2 to the best of the authors’ knowledge. With reference to Fig. 2, if a user is engaged in an Across Air session, her personal data flows can easily go across 4 different proprietary platforms. A useful privacy machine agent could summarize all the policies for the users and match the user’s preferences to preserve important privacy properties, e.g. the 7Cs, such as user comprehension and consciousness, and to facilitate user consent and choice in context [3].

Focus on Software Engineers and Users

Obtaining answers to the above issues requires design thinking in holistic, interdisciplinary, and innovative ways. Employing considerable multidisciplinary design experience, spanning from policy to business to technology, the OASIS PbD-SE TC [6] focuses on the software engineering stakeholder as he/she impacts the user in many ways, including leading the next generation technologies that users adopt. The PbD-SE produces a methodology for software engineers to use as a guide to embed and document their compliance to Privacy by Design (PbD) principles [2]. Outputs of the methodology document privacy requirements from policy environment to software conception to retirement, thereby providing a plan around compliance to PbD, and alignment to other guidance such as the NIST’s 800-53 Appendix J, the Fair Information Practice Principles (FIPPs), and the Generally Accepted Privacy Principles (GAPP).

The PbD-SE TC’s major approach is to treat privacy requirements as functional requirements that should be scoped out at the same time that the Augmented Reality application, or whatever software application, is specified. The PbD-SE specification references its sister OASIS PMRM [7] specification at the use case/user story level to obtain sophisticated privacy requirements at multiple levels. Once privacy requirements are documented, tests for privacy preservation may be conveniently written at the same time that software tests are written for the implementation of functional specifications. Other steps are laid out in the PbD-SE methodology.

Some of the documentation that software engineers may access internally may include business models, e.g. as illustrated in Fig. 2, that show personal data flows among stakeholders and platforms. Such diagrams help software engineers to clearly visualize personal data flow, and data ownership issues at a macro level before they get down in the weeds. While remaining agnostic to choice of modeling language, the PbD-SE TC uses the OMG software modeling standard UML, and other popular representation languages and tools, including and not limited to, data flow diagrams (DFDs) and spreadsheet modeling, to provide concrete examples of documentation.

Building a Mainstream Privacy Engineering Toolset as a Tourniquet

It is possible that new business models involving privacy will emerge. For example, “trusted” corporations in regulated industries, such as financial services, with deep experience in managing risks around customer identity may eventually step up to store our big expensive personal clouds. These corporations, or networks, may conduct permission-based transactions on our behalf with machine agents, and other customers. Policymakers and technologies may address the aggregation risk in future. But in the meantime, we need a robust tourniquet to stop the bleeding around our privacy.

As a start, it is not difficult to build tools for educators to train software engineers to easily visualize privacy requirements for their mobile AR, IoT, or other software apps. Software tools used by software engineers to communicate software requirements currently include UML modelers, spreadsheets, and text documents. UML modelers are commonly found in both paid (e.g., Visio), and open source (e.g., Eclipse) formats. UML extensions [4], which may be implemented as stereotypes, will also be useful for visualization of privacy specifications. For instance, Fig. 2 is an example snapshot of a tool screen to teach software engineers to add Notice, Usage, Agreement Services, and other privacy requirements as services to their functional specifications.
Summary
Advances in AR and the IoT hold a lot of promise for ubiquitously empowering underserved users, such as people with disabilities [5], but these technology-enabled environments also exponentially exacerbate a loss of privacy. Our position talks to the need for preserving the users’ 7Cs, treating privacy requirements as functional requirements versus quality attributes, desire for privacy-respecting business models, and social need for all industry sectors to accept and embrace privacy standards. We champion a focus on tools for the software engineer and the software organization in privacy standards. We further suggest using extended UML-based toolkits to assist in moving privacy engineering education to the software engineering mainstream. A lot of work is still required to close the loop, if we want to build inclusive societies, where we are empowered by augmented reality and IoT apps, and where our privacy is protected simultaneously by default and by design.

References
[8] The Platform for Privacy Preferences (P3P), http://www.w3.org/P3P/