Participatory Design Research to Understand the Legal and Technological Perspectives in Designing Health Information Technology

Extended Abstract[†]

M. Aljohani
Faculty of Computer Science
Dalhousie University
Canada
mh578194@dal.ca

J. Blustein
Faculty of Computer Science
Dalhousie University
Canada
Jamie@cs.dal.ca

K. Hawkey
Faculty of Computer Science
Dalhousie University
Canada
Hawkey@cs.dal.ca

ABSTRACT

In this paper, we report applying participatory design research on the development of effective privacy compliance framework in the context of healthcare applications provided to IT designers. We aim to bridge the gap between privacy law designers and privacy IT designers by expanding the concept of end-user participation. We propose a mixed approach between Participatory Design Research and Human Computer Interaction techniques to facilitate the participation of different stakeholders during the design lifecycle.

CCS CONCEPTS

• **Human-centered computing → Participatory design**; • **Empirical studies in HCI** • **User studies → Interview** • **User centered design**

KEYWORDS

Privacy; Privacy legislations; Personal Health Information; e-Health; Patient Portals; Electronic Health Records; Electronic Medical Records; Personal Health Records.

1 INTRODUCTION

The increasing number of privacy laws of personal health information has motivated our research in integrating laws requirements as design requirements. Privacy in Canada is regulated under two main Acts: The *Privacy Act*, which deals with personal information and how it is handled by organizations; and the *Personal Information Protection and Electronic Documents Act* (PIPEDA), which covers "the federal private-sector privacy law" that deals with the use and disclosure of personal information in commercial activities in Canada [1]. Applying the privacy rules in Information Technology is challenging. The literature is lacking in methods and techniques on integrating privacy law requirements as design requirements [2]. We propose a Participatory Design Research approach to provide IT designers with effective privacy compliance framework in the context of healthcare applications.

SIGDOC '17, August 11–13, 2017, Halifax, NS, Canada

ACM ISBN 978-1-4503-5160-7/17/08…$15.00
https://doi.org/10.1145/3121113.3121240

1.1 Gap between Law and Technology

There is a need to bridge the gap between privacy laws and privacy IT design [3][4][5]. The underlying problem behind the lack of privacy framework compliance in the literature is due to the gap between privacy designers from both the legal and technological perspectives. The reasons behind the existing research problems include: it is difficult to fully capture the legal requirements and integrate them as design requirements because of the way they are formed "technology neutral" [3][4][5]. Second, privacy designers (legal representatives) and IT designers (IT representatives) do not communicate; they "do not understand each others disciplines; very few lawyers are trained software engineers and vice versa" [6]. The third reason is the lack of focus on the "process". The research and legal documentation lack stating [how] the privacy laws can be enforced in the digital world [6]. Our proposed solution is to bring these two professions together and provide IT designers with a one-stop shop of methodologies and a research framework that shows how to comply with legal requirements.

2 PARTICIPATORY DESIGN RESEARCH

"Participation [is how] stakeholders – especially users, developers and planners – cooperatively make or adjust systems, technologies and artifacts in ways which fit more appropriately to the needs of those who are going to use them." [7]. We are motivated to focus on applying methods of Participatory Design (PD) research because there is a need for interdisciplinary knowledge exchanges from different stakeholders. PD is a process that involves different stakeholders working together to design a solution. PD "can lead to hybrid experiences – that is, practices that take place neither in the users' domain, nor in the

technology developers' domain, but in an "in-between" region that shares attributes of both spaces" [8].

2.1 Research Objectives

The main research area is the interaction between three professions: using Personal Health Information Act (PHIA) as a case to represent the privacy laws and applying the Participatory Design research in the context of e-Health as an online patient portal. The main objective is to form privacy-preserving design guidelines based on privacy laws by applying participatory design research approaches. A supporting goal is to take the first step toward bridging the gap between IT designers and Law representatives by applying a mixed approach between PD and HCI techniques

2.2 Methodology Model

The proposed PD research approach is divided into five phases as shown in Fig. 1. Starting from analyzing PHIA as a case representing privacy laws to propose privacy patterns, which then used for the thematic analysis. The requirement-gathering phase aims to collect qualitative data from different stakeholders to draw a complete picture of current practices, challenges, knowledge, experience, perception and future recommendation of managing Electronic Health Records (EHRs) in general and through online portals as the first research phase. Next steps include cooperative prototyping that aims to support different stakeholders in the design process including privacy laws representatives and technology representatives. In the final phase, a cooperative evaluation of a proof-of-concept privacy preserving designs will be evaluated by law representatives, technology representatives and end users (patients).

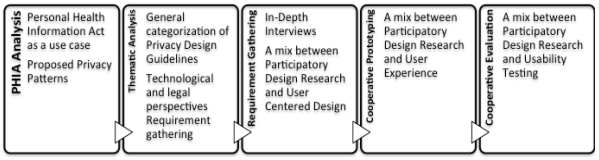

Figure 1. Participatory Design Research approach

2.2.1 PHIA analysis and Thematic Analysis

We have proposed privacy patterns based on Nova Scotia's Personal Health Information Act (PHIA) [2]. The following five proposed privacy patterns are 1-request an access 2-request a correction 3-request not to disclose Personal Health Information 4-being notified if the PHI is lost, stolen or subject to unauthorized access 5-request a review. The patterns provide a guide to designers and developers in designing privacy-preserving systems in healthcare [2].

The Thematizing Analysis stage relies mainly on the analysis of patients' privacy rights proposed in [2]. The analysis focuses on providing detailed understanding of each patient's privacy right under PHIA and privacy patterns (guidelines) were proposed to cover privacy rights based on PHIA.

2.2.2 Mapping to Privacy International Standards

The validation of the proposed patterns was motivated to generalize the proposed patterns by mapping them to international and standardized-based approaches, which help to answer the question: what privacy principles are guaranteed if the system design follows the proposed patterns?

We mapped the patterns to ISO 29100 Privacy Framework [9] and Process Oriented Strategies [10]. The mapping process included 10 general principles and 38 sub-principles. We found that 19 privacy principles were fully covered and five were partially covered. Six principles were not mapped and we refined pattern P3: request not to disclose and P4: being notified patterns. We found that the proposed pattern fully covered the Process Oriented Strategies or Privacy-by-Policy.

2.2.3 Preliminary Categorization

We have combined the rules of PHIA and the results from the mapping process to create a general categorization. The general categorization is shown in Fig. 2 includes data access, consents, data collection, notification, and privacy preferences. The implementation of PHIA is discussed in the current practices to cover challenges, knowledge, experience, perception and future recommendation of managing EHRs in general and through online portals.

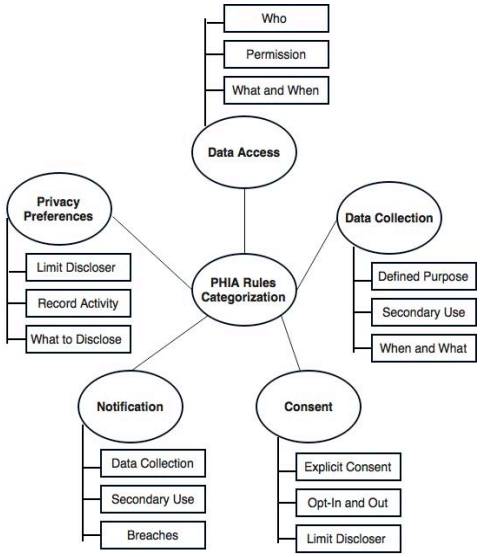

Figure 2. PHIA rules categorization

These categories were used to form the In-depth Interview and will be refined to form the design guidelines as we proceed with the research plan. The interviews are planned to target different stakeholders, who are considered to be PHIA users, to cover both the legal and technological perspectives, which is the current research phase.

2.3 Potential Contributions

Effective privacy compliance framework in the context of healthcare applications provided to IT designers to bridge the gap between privacy laws and privacy IT design. We propose expanding the concept of end-user participation to include not only end-users but all stakeholders who could have influence on the design process during the design lifecycle. The potential contribution represents a mixed approach between Participatory Design Research and Human Computer Interaction techniques to facilitate the participation of different stakeholders during the design lifecycle.

ACKNOWLEDGMENTS

This work was funded by University of Jeddah in Saudi Arabia, with the support of the Saudi Cultural Bureau in Canada. The authors appreciate and acknowledge the support given by these organizations.

REFERENCES

[1] Office of the privacy commissioner of Canada (2014). Overview of privacy legislation in Canada. Retrieved From: https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

[2] Aljohani, M., Hawkey, K., & Blustein, J. (2016, July). Proposed Privacy Patterns for Privacy Preserving Healthcare Systems in Accord with Nova Scotia's Personal Health Information Act. In International Conference on Human Aspects of Information Security, Privacy, and Trust (pp. 91-102). Springer International Publishing.

[3] Compagna, L., El Khoury, P., Krausová, A., Massacci, F., & Zannone, N. (2009). How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns. Artificial Intelligence and Law, 17(1), 1-30.

[4] Swire. P., & Anton, A., Engineers and Lawyers in Privacy Protection: Can We All Just Get Along? *Privacy Perspectives.* (January 13, 2014). Accessed (August, 2016). Retrieved From: https://iapp.org/news/a/engineers-and-lawyers-in-privacy-protection-can-we-all-just-get-along/

[5] Canada's Health Informatics Association. (2012). *Privacy for patient portals: 2012 guidelines for the protection of health information.* Retrieved from http://www.ehealthontario.on.ca/images/uploads/pages/documents/Privacy- Security-for-Patient-Portals.pdf

[6] Oliver, I., On Finding Reasonable Measures To Bridge the Gap Between Privacy Engineers and Lawyers. *Privacy Perspectives. (July 29*, 2014). Accessed (August, 2016). Retrieved From: https://iapp.org/news/a/on-finding-reasonable-measures-to-bridge-the-gap-between-privacy-engineers-and-lawyers/

[7] Robertson, T., & Simonsen, J. (2012). Participatory Design. *Routledge international handbook of participatory design*, 1.

[8] Muller, M. J. & Druin, A. (2003). Participatory design: the third space in HCI. Human-computer interaction: Development process, 4235, 165-185.

[9] ISO/IEC 29100. Information technology – Security techniques – Privacy framework. Technical report, ISO JTC 1/SC 27

[10] Hoepman, J. H. (2014). Privacy design strategies. In ICT systems security and privacy protection (pp. 446-459). Springer Berlin Heidelberg.