

Chapter 12

The Unheard Story of Organizational Motivations Towards User Privacy

Awanthika Senarath

University of New South Wales, Australia

Nalin Asanka Gamagedara Arachchilage

The University of New South Wales, Australia

ABSTRACT

There could be numerous reasons that drive organizations to provide privacy protections to end users in the applications they develop and maintain. Organizational motivations towards privacy affects the quality of privacy received by end users. Understanding these motivations and the approaches taken by organizations towards privacy protection would assist the policymakers and regulators to define effective frameworks encouraging organizational privacy practices. This study focuses on understanding the motivations behind organizational decisions and the approaches they take to embed privacy into the software applications. The authors analyzed 40 organizations different in size, scope, scale of operation, nature of data used, and revenue. they identified four groups of organizations characterized by the approach taken to provide privacy protection to their users. The taxonomy contributes to the organizational perspective of privacy. The knowledge presented here would help addressing the challenges in the domain of user privacy in software applications and services.

INTRODUCTION

With the pervasiveness of information technology, connected applications that continuously collect user data have become indispensable in modern life (Shapiro, 2016). Users heavily depend on organizations that develop and publish software applications to protect an enormous amount of personal data disclosed, such as locations, personal schedules, identification and financial information and even blood types and

DOI: 10.4018/978-1-5225-9742-1.ch012

glucose levels (Ginosar & Ariel, 2017). This impose a huge responsibility and risk on the organizations that collect, store and process user data in their businesses to uphold the trust extended by end users on their data practices.

Privacy experts and privacy-concerned users are continuously demanding for better privacy through ubiquitous systems such as on-line sales, banking, social networking applications, mobile phones and telecommunication services (Sarvas & Frohlich, 2011). Research community in the field of privacy and security are implementing methodologies for organizations to follow, in embedding privacy into the systems they develop (Langheinrich, 2001) (Wright & De Hert, 2012). Governments and legal authorities are pushing organizations to comply with rules and regulations defined to protect end user privacy (Fromholz, 2000). However, for the success of all of the aforementioned attempts this research aims to address the following research questions,

- What motivate organizations, to embed privacy into the software systems they develop and on-line services they provide?
- Driven by these motivations, what are the approaches taken by organizations to embed privacy into the systems they develop and maintain?

Organizations that deal with personal information of users differ significantly in size, scope, scale of operation, field of operation, nature of data stored and used, and by the revenue they make. It is estimated that the volume of user data stored in Facebook would be measured in zeta-bytes by 2020 (Anthonysamy, Rashid, & Chitchyan, 2017), which cannot even compare to the amount of data handled by small-scale companies. Anecdotal evidence suggest that such differences in organizational structures and backgrounds, affect their approach towards end user privacy. Nevertheless, Ginosar and Ariel (Ginosar & Ariel, 2017) emphasize that an interpretation of privacy from an organizational aspect has been missing from the privacy research approaches taken so far. Understanding this gap is critical because, as Brunton and Nissen (Brunton & Nissen, 2017) claim, “In the digital economy, the real power is not held by individual consumers and citizens using their smart-phones and laptops to navigate the twists and turns of their lives, but by the large government and corporate entities who monitor them”.

Driven by these motivations, we scrutinized 40 organizations that deal with user data. Our study revealed interesting aspects as to how different organizations see and perceive user privacy within their business practices. Further, we define a taxonomy of privacy protection approaches adopted by organizations based on the motivation they have towards end user privacy. Based on our taxonomy we provide implications for businesses, governments and researchers to consider in establishing privacy frameworks, regulations and policies.

Our work contributes to the knowledge of organizational perspective on privacy in the governing and regulating authorities that define and enforce privacy regulations. Findings of this study would also help the research community to identify how to communicate their research and proposals on privacy methodologies, and guidelines effectively to target organizations. Through this work we invite the research community and national and sectoral bodies (Ginosar & Ariel, 2017) to focus on providing tailor made privacy solutions for businesses operating on different types of personal data for different business motives and purposes, in different scales and business models.

The paper is structured as below. The related work extensively elaborate on work done so far in identifying organizational characteristics pertaining to their decisions and approaches towards privacy. Research methodology section contains information on our study approach followed by the results. In

22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:
www.igi-global.com/chapter/the-unheard-story-of-organizational-motivations-towards-user-privacy/234815

Related Content

The Impacts of Risk on Deploying and Sustaining Lean Six Sigma Initiatives

Brian J. Galliand Mohamad Amin Kaviani (2018). *International Journal of Risk and Contingency Management* (pp. 46-70).

www.irma-international.org/article/the-impacts-of-risk-on-deploying-and-sustaining-lean-six-sigma-initiatives/191219

Reversible Data Hiding Scheme for Video

T. Bhaskarand Madhu Oruganti (2019). *International Journal of Information Security and Privacy* (pp. 1-13).

www.irma-international.org/article/reversible-data-hiding-scheme-for-video/226946

(p+, , t)-Anonymity Technique Against Privacy Attacks

Sowmyarani C. N., Veena Gadadand Dayananda P. (2021). *International Journal of Information Security and Privacy* (pp. 68-86).

www.irma-international.org/article/p--t-anonymity-technique-against-privacy-attacks/276385

Metamorphic malware detection using opcode frequency rate and decision tree

Mahmood Fazlali, Peyman Khodamoradi, Farhad Mardukhi, Masoud Nosratiand Mohammad Mahdi Dehshibi (2016). *International Journal of Information Security and Privacy* (pp. 67-86).

www.irma-international.org/article/metamorphic-malware-detection-using-opcode-frequency-rate-and-decision-tree/160775

Data Controller, Processor, or Joint Controller: Towards Reaching GDPR Compliance in a Data- and Technology-Driven World

Yordanka Ivanova (2020). *Personal Data Protection and Legal Developments in the European Union* (pp. 61-84).

www.irma-international.org/chapter/data-controller-processor-or-joint-controller/255193