GRES-IT Workshop Proceedings
Proceedings Editors: Barbara Krumay, Roman Brandtweiner

Arbeitspapiere zum Tätigkeitsfeld Informationsverarbeitung, Informationswirtschaft und Prozessmanagement
Working Papers on Information Systems, Information Business and Operations

Nr./No. 02/2016
ISSN: 2518-6809
URL: http://epub.wu.ac.at/view/p_series/S1/

Herausgeber / Editor:
Department für Informationsverarbeitung und Prozessmanagement
Wirtschaftsuniversität Wien - Welthandelsplatz 1, 1020 Wien
Department of Information Systems and Operations
Vienna University of Economics and Business – Welthandelsplatz 1 · 1020 Vienna
Taking Responsibility for Online Self-disclosure
The thin line between a company’s user orientation and user surveillance

Christine Bauer
University of Vienna
Department of eBusiness
Vienna, Austria
chris.bauer@univie.ac.at

Companies using the Internet for their business to consumers (business-to-consumer; B2C) frequently require users to disclose personal information (PI). For instance, for establishing legitimacy [e.g., 1] or authentication [e.g., 2, 3] users have to confirm their identity. For online sales, the user has to disclose PI such as full name, address, and credit card details for payment and fulfilling invoicing requirements [3, 4]. User profiles (based on user characteristics and/or behavior) are necessary for offering personalized services that are tailored to the individual (e.g., recommender systems [5]) [2, 6]. Similar user profiles are required for better targeting advertising campaigns [7]. What is more, online social networks (e.g., Facebook) and other social media services would be nonexistent without having users disclosing PI [8]; providers of such services build their entire business on users’ self-disclosure. In a nutshell: users’ online self-disclosure (OSD) is highly valuable for companies, allowing the latter offering their services and running effective marketing campaigns.

However, for users it is not always favorable to provide PI openly. In fact, revealing too much PI may be problematic [9-11]: The digital availability of PI facilitates copying, transmitting, and integrating such information easily, and the exploitation of PI could, thus, result in serious threats which can be both financial and social if in the wrong hands [9, 10, 12-14]. Aware of these threats, users attempt to “hold back” some PI to maintain the level of privacy that they wish to maintain [15]; they struggle in finding their balance in the tension between their desire to self-disclose and the desire to protect themselves [16].

Still, users’ self-disclosing behavior is manipulable. For instance, Bauer and Schifffinger [17] found that system-based variables, such as system functionality and usefulness, have a substantial impact on OSD and are at least moderately effective. This fact would allow companies to purposefully “shape” users’ self-disclosure. In short, companies could use system design to either manipulate users to disclose less or more PI.

But what is the role of the company in this context? Is it morally okay to exploit users’ PI for their own profit? Or do companies have the responsibility to remunerate users whose PI they exploit? Do companies have the responsibility to protect users from self-disclosing too much?

There are two sides. One side supports that companies have to respect the users’ desire for privacy and cannot collect and exploit at all their PI for the companies’ profit. The other side claims that if users give away their PI abundantly and freely (e.g., on online social networks), why not use it; those that do not want to provide their PI should not use the offered service. Total surveillance and full privacy are the two extreme poles, of course. Hybrid forms are possible and currently reality.

But how should a company decide what to do? Several strategies are conceivable:

- **Privacy by design:** Privacy by design – an example of value-sensitive design – is an approach to systems engineering that takes privacy into account throughout the entire engineering process [18]. This approach has, though, been critiqued for being vaguely defined, leaving open questions in how to apply this approach when engineering systems [19].

- **Situationalization:** Situationalization [20] refers to using information characterizing the present situation based entirely on (physical) context that is not related to an individual or group of individuals (non-personal aspects); examples are location, time, atmospherics, or the social environment. In contrast to personalization, situationalization eliminates the need for person-related data (i.e., PI) [7]. As a result, this approach does not require users to self-disclose. And besides being privacy-sensitive, it may even be more effective than a personalization strategy [7].

- **Privacy seal:** Another strategy is to provide a privacy indicator, statement, or seal to informs users about the privacy efforts of that company [21]; this strategy may be used in addition to privacy by design or a situationalization approach. Privacy seals have, though, been reported as having only moderate effects on self-disclosure [22]. A responsible company will never show a privacy seal or statement to its users and not adhering to the stated policies.

- **Transparency on PI use:** Collecting and leveraging users’ PI and clearly informing them – in advance – about data use is another strategy that companies may follow. The problem with current practice is that many companies have long data policy statements that are
little informative and/or hide the relevant statements on PI processing. A company taking the responsibility role seriously will definitely put effort in making their policy transparent and understandable to the average user.

Service duality: Another strategy could be to offer two systems/services with different functionality, so that users with different attitudes towards self-disclosure and PI use may be served with different systems/services. Although this duality in service offering implies additional costs, these costs may be balanced by service pricing: Some people may pay for maintaining their privacy, whereas others may pay a higher fee for getting access to additional features in exchange for providing more PI to the company. This will potentially lead to the same (higher) price for the service for both user groups.

While this work-in-progress cannot provide answers to how a company may decide on the preferred strategy, the above non-exhaustive enumeration offers an overview of available options. Further research is necessary for investigating both the feasibility and impact of the various strategies.

REFERENCES


