WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

EFMD EQUIS ACCREDITED

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 Schiffinger [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

[1] J. Galegher, L. Sproull, and S. Kiesler, "Legitimacy, authority, and community in electronic support groups," *Written Communication,* vol. 15, no. 4, pp. 493-530, Oct 1998.

[2] A. N. Joinson, C. Paine, T. Buchanan, and U.-D. Reips, "Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys," *Computers in Human Behavior,* vol. 24, no. 5, pp. 2158-2171, Sep 2008.

[3] M. J. Metzger, "Effects of site, vendor, and consumer characteristics on web site trust and disclosure," *Communication Research,* vol. 33, no. 3, pp. 155-179, Jun 2006.

[4] M. J. Metzger, "Privacy, trust and disclosure: exploring various barriers of e-commerce," *Journal of Computer-Mediated Communication,* 2004.

[5] F. Ricci, L. Rokach, and B. Shapira, *Recommender systems handbook*, 2nd ed. Boston, MA: Springer, 2015.

[6] E. B. Andrade, V. Kaltcheva, and B. Weitz, "Self-disclosure on the web: The impact of privacy policy, reward, and company reputation," *Advances in Consumer Research,* vol. 29, pp. 350-353, 2002.

[7] C. Bauer and P. Lasinger, "Adaptation strategies to increase advertisement effectiveness in digital media," *Management Review Quarterly,* vol. 64, no. 2, pp. 101-124, April 2014.

[8] S. Trepte and L. Reinecke, "The effects of social network use on privacy, social support, and well-being: A longitudinal study," in *3rd European Communication Conference (ECREA 2010)*, Hamburg, Germany, 2010.

[9] Y. Al-Saggaf and S. Nielsen, "Self-disclosure on Facebook among female users and its relationship to feelings of loneliness," *Computers in Human Behavior,* vol. 36, pp. 460-468, Jul 2014.

[10] V. Kisekka, S. Bagchi-Sen, and H. R. Rao, "Extent of private information disclosure on online social networks: an exploration of Facebook mobile phone users," *Computers in Human Behavior,* vol. 29, no. 6, pp. 2722-2729, Nov 2013.

[11] A. Acquisti, L. Brandimarte, and G. Loewenstein, "Privacy and human behavior in the age of information," *Science,* vol. 347, no. 6221, pp. 509-514, Jan 2015.

[12] A. Nosko, E. Wood, and S. Molema, "All about me: Disclosure in online social networking profiles: The case of FACEBOOK," *Computers in Human Behavior,* vol. 26, no. 3, pp. 406-418, May 2010.

[13] S. Mukherjee, J. A. Manjaly, and M. Nargundkar, "Money makes you reveal more: consequences of monetary cues on preferential disclosure of personal information," *Frontiers in Psychology,* vol. 4, p. 839, 2013.

[14] N. K. Malhotra, S. S. Kim, and J. Agarwal, "Internet users' information privacy concerns (IUIPC): Tthe construct, the scale, and a causal model," *Information Systems Research,* vol. 15, no. 4, pp. 336-355, Dec 2004.

[15] J. Shibchurn and V. Xiang Bin, "Investigating Effects of Monetary Reward on Information Disclosure by Online Social Networks Users," in *47th Hawaii International Conference on System Sciences (HICSS 2014)*, Big Island, HI, 2014, pp. 1725-1734: IEEE.

[16] M. Taddicken, "The 'privacy paradox' in the social web: The impact of privacy concerns, individual characteristics, and the perceived social relevance on different forms of self-disclosure," *Journal of Computer-Mediated Communication,* vol. 19, no. 2, pp. 248-273, Jan 2014.

[17] C. Bauer and M. Schiffinger, "Self-disclosure in online interaction: a meta-analysis," in *48th Hawaii International Conference on System Sciences (HICSS 2015)*, Kauai, HI, 2015, pp. 3621-3630: IEEE.

[18] P. Hustinx, "Privacy by design: delivering the promises," *Identity in the Information Society,* vol. 3, no. 2, pp. 253-255, Aug 2010.

[19] J. van Rest, D. Boonstra, M. Everts, M. van Rijn, and R. van Paassen, "Designing Privacy-by-Design," in *Privacy Technologies and Policy: First Annual Privacy Forum, APF 2012, Limassol, Cyprus, October 10-11, 2012, Revised Selected Papers*, B. Preneel and D. Ikonomou, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2014, pp. 55-72.

[20] P. Lasinger and C. Bauer, "Situationalization: the new road to adaptive digital-out-of-home advertising," in *IADIS International Conference e-Society 2013 (ES 2013)*, Lisbon, Portugal, 2013, pp. 162-169: IADIS.

[21] B. P. Knijnenburg and A. Kobsa, "Making Decisions about Privacy: Information Disclosure in Context-Aware Recommender Systems," *ACM Transactions on Interactive Intelligent Systems,* vol. 3, no. 3, pp. 1-23, 2013.

[22] N. J. Rifon, R. LaRose, and S. M. Choi, "Your privacy is sealed: effects of web privacy seals on trust and personal disclosures," *Journal of Consumer Affairs,* vol. 39, no. 2, pp. 339-362, Win 2005.