Editorial 25/2: Electronic Markets and privacy

Rainer Alt¹ · Carsta Militzer-Horstmann¹ · Hans-Dieter Zimmermann²

Published online: 14 May 2015

© Institute of Information Management, University of St. Gallen 2015

Dear readers of Electronic Markets,

The aspect of privacy is a current and at the same time an established topic for electronic markets. In its first issue of 2015, Science magazine featured a special theme titled “The End of Privacy” (Enserink and Chin 2015), which was motivated by the need to find a balance between protecting private data on the one hand and making it available for desired uses on the other. While data on individuals and/or organizations is necessary for providing value-adding information services, such as monitoring, analyzing or tracking data for health, transactional or other behavioral purposes, the “right to be left alone” is still posited a valuable good in itself (e.g. Berendt et al. 2005, p. 101). However, keeping private data private is increasingly becoming a challenge: Recent research shows that even if data is anonymized, linking multiple anonymous data points enables algorithms to re-identify the “underlying” individual or organization (de Montjoye et al. 2015). The tradeoff between both contrary developments has also been referred to as “personalization-privacy paradox” (Sutanto et al. 2013), but in addition to the fact that users are concerned about breaches of their privacy, this problem is more often also a problem of trust (Strathoff and Lutz 2014). Platform and service operators are regarded as unreliable actors who

are not transparent and use data for unauthorized or unintended purposes. This means that information hubs, such as electronic markets, play a key role in this race between protecting information and making it selectively available for desired uses (see Fig. 1):

- First, electronic intermediaries are providers of (cloud) services that link multiple actors in value chains, such as buyers and sellers, and should ensure a minimum level of security on the infrastructural, i.e. data access and transfer level. In the business-to-consumer domain, widespread encryption-based technologies used for accessing services are Https and SSL, while in the business domain dedicated networks (e.g. SITA in the airline industry or ENX in the automotive industry) have emerged to offer higher levels of security. The goal is to create data and, in the case of electronic markets, a transaction environment enabling secure access and storage of (transaction and identity) data as well as the governance of personal data (e.g. who is allowed to see, modify and/or delete data and under which regulations).
- Second, electronic markets are not limited to providing a secure environment, but also need to address how the participating actors (i.e. sellers and buyers) use this infrastructure. Usually, transactions for goods and services on electronic markets comprise functionalities for information, contracting and settlement activities. Among the examples for these (primary) business transactions are information and comparison searches as well as ordering in a multi-vendor catalog or an auction platform. The intermediary facilitates transactions and privacy measures may ensure that data collected prior, during and after the transactions is kept private and not made available for other (marketing) purposes, such as cross-selling. For example, airline reservation systems are similar to

✉ Rainer Alt
rainer.alt@uni-leipzig.de

Carsta Militzer-Horstmann
militzer-horstmann@wifa.uni-leipzig.de

Hans-Dieter Zimmermann
hansdieter.zimmermann@fhsg.ch

¹ Information Systems Institute, University of Leipzig,
Grimmaische Str. 12, 04109 Leipzig, Germany

² FHS St. Gallen, University of Applied Sciences,
Rosenbergstrasse 59, 9001 St. Gallen, Switzerland

Fig. 1 Levels of privacy in electronic markets

search engine providers who generate knowledge from the searches and the user behavior on their platform. Since many transactions are complex and represent bundles of individual products, the classical passenger name records have been enhanced to become so-called “Total Travel Records”, which not only comprise data from flights, but also from hotels, restaurants or concert ticket agencies (Boehmer 2013). Obviously, this has the potential to make customers more transparent and in case of privacy breaches the reputation or integrity of a person or organization can be seriously damaged.

- Third, data also emerges from the activities on the electronic market platform itself and may be used for secondary transactions. Service providers and intermediaries have accumulated detailed data on individuals from the bookings made via the platform and algorithms as mentioned above are helpful for deriving knowledge on individual user behavior and preferences as well as on collective developments, such as evolving trends or causalities and correlations. For example, selling anonymized data on aggregated transactions, customer (segments) and the like are established services by marketplace operators (e.g. Alexa by Amazon). Obviously, the transparency on how these data are re-used remains even more obscure for consumers, and mechanisms to control this universe of potential uses are still open fields of research. They could also offer interesting opportunities for (new) intermediaries and electronic markets for personal data as discussed in the present special issue are an important contribution to this debate.

The three levels illustrate that inappropriate handling of (personal) data in the electronic market environment may have severe consequences for the marketplace participants and in particular regarding the trust in the marketplace operator. An analysis of past articles published in *Electronic Markets* reveals that this relationship between trust and privacy has repeatedly been a topic in our journal since 2001. However, the 25 papers that were identified mainly focused on the first levels of privacy (see Table 1):

- The issues discussed on level 1 include a proposal of a fair and privacy-preserved protocol for sealed-bid auctions (Liao and Hwang 2001), a privacy-aware decision engine (Gogoulos et al. 2014) or a digital rights management scheme for Web services in e-commerce (Kwok et al. 2003). Research also addressed the impact of perceived privacy empowerment (van Dycke et al. 2007) as well as privacy issues in the era of ubiquitous commerce (Galanxhi and Nah 2006; Loebbecke 2007) and the “Internet of things” (Xu and Gupta 2009), where additional privacy concerns arise due to the availability of location-based information from various mobile technologies (e.g. RFID tags, smartphones).
- Research on level 2 mainly investigated contingencies determining the emergence of trust among the participating parties and, in particular, the trust towards the website or market provider. Online trust has been viewed as the result of privacy and security measures (Riquelme and Román 2014) and has been recognized as an important factor for the continued use of electronic platforms (Sun et al. 2014; Becker et al. 2008). Early insights on trust-building elements, such as privacy seals and reputation advertising, have been suggested by McKnight et al. (2004), while Saeed and Leitch (2003) propose a framework for assessing the sourcing risk. Transparent communication on how data are secured and the availability of adequate legislation has also been emphasized in the area of mobile commerce (see O’Reilly et al. 2012).
- Some indications on the relevance of level 3 were provided in the first special issue that was dedicated to “Security and privacy in business networking” (Wohlgemuth et al. 2014). The guest editors coined the vision of “making business processes resilient” and one contribution recognized that the “collection, processing, and selling of personal data is an integral part of today’s electronic markets” (Kieseberg et al. 2014, p. 113). It suggested an anonymization algorithm that might be used as an infrastructural element for these purposes.

Table 1 Articles on security and privacy published in Electronic Markets

Vol./Iss.	Article title	Level 1	Level 2	Level 3
24/2	Is the influence of privacy and security on online trust the same for all type of consumers?		x	
24/2	Security and privacy in business networking	x		x
24/2	Secure provision of patient-centered health information technology services in public networks	x		
24/2	On the design of a privacy aware authorization engine for collaborative environments	x		
24/2	An algorithm for collusion-resistant anonymization and fingerprinting of sensitive microdata	x		x
24/2	Take care of your belongings today – Securing accessibility to complex electronic business processes	x		
24/2	Understanding Chinese user's continuance intention towards online social networks: An integrative theoretical model		x	
23/4	Change factors in Enterprise 2.0 initiatives: Can we learn from ERP?	x		
22/4	To M-Pay or not to M-Pay - Realising the potential of smart phones: conceptual modelling and empirical validation		x	
22/3	Mobile advertising avoidance: Exploring the role of ubiquity		x	
21/4	Online buying perceptions in Spain: Can gender make a difference?		x	
19/2-3	The effects of privacy concerns and personal innovativeness on potential and experiences customer's adoption of location-based services		x	
18/4	Inclusive electronic public service delivery – A quantitative analysis	x	x	
17/1	Piloting RFID along the supply chain: A case analysis	x		
17/1	The effect of consumer privacy empowerment on trust and privacy concerns in E-commerce	x		
16/3	Privacy issues in the era of ubiquitous commerce	x		
16/1	The attraction of Internet personalization to web users	x		
14/4	Distrust of one's own web skills: A reason for offline booking after online information search		x	
14/4	Information assurance in B2C websites for informations good/services		x	
14/3	Continuous trading in thin private value markets: The multiple-quote double auction	x		
14/3	Shifting factors and the ineffectiveness of third party assurance seals: A two-stage model of initials trust in a web business		x	
13/2	Digital rights management in web services	x		
13/2	Controlling sourcing risk in electronic marketplaces		x	
11/3	A fair and privacy-preserved protocol for sealed-bid auctions	x		
11/2	Contrasting European and American approaches to privacy in electronic markets: Property rights versus civil right	x		

The present issue of Electronic Markets provides more insights on personal data markets, which may be viewed as a development on level 3. We are indebted to the team of guest editors (Sarah Spiekermann from Vienna University of Economics and Business, Alessandro Acquisti from Carnegie Mellon University, Rainer Böhme from Westfälische Wilhelms Universität Münster, and Kai-Lung Hui from The Hong Kong University of Science and Technology), who managed to organize a comprehensive issue for a highly relevant topic. It not only includes three research articles, but also an invited paper from practice (Maguire et al. 2015) and a position paper by the guest editors themselves, which adds to the understanding of the problem of personal data markets and on how the field might develop (Spiekermann et al. 2015b). As usual, the guest editors will introduce all five special issue papers in their preface (Spiekermann et al. 2015a). We hope you enjoy reading these articles!

Last but not least, we are happy that Electronic Markets has improved its position in one of the most important rankings in the German-speaking area. While the earlier Jourqual 2.1 ranking listed Electronic Markets as “C”, it is now ranked “B” in Jourqual 3 (JOURQUAL3, 2015). Needless to say, the voting reflects the continued effort of all members of the Electronic Markets' community – readers, authors, reviewers and our members of the editorial board. We wish to take the opportunity to express our gratitude for your effort and hope that you support us in making Electronic Markets an even more valuable source for scholars as well as practitioners in the future.

Best regards from Leipzig and St. Gallen,

Rainer Alt, Carsta Militzer-Horstmann, Hans-Dieter Zimmermann

References

- Becker, J., Niehaves, B., Bergener, P., & Räckers, M. (2008). Inclusive electronic public service delivery - A quantitative analysis. *Electronic Markets*, 18(4), 315–323. doi:10.1080/10196780802420687.
- Berendt, B., Günther, O., & Spiekermann, S. (2005). Privacy in E-commerce: Stated preferences vs. Actual behavior. *Communications of the ACM*, 48(4), 101–106.
- Boehmer, J. (2013). Amadeus moving beyond PNR with “total travel record”. *Business Travel News*, 30(12), 38.
- De Montjoye, Y.-A., Radaelli, L., Singh, V. K., & Pentland, A. (2015). Unique in the shopping mall: on the reidentifiability of credit card meta-data. *Science*, 347(6221), 536–539. doi:10.1126/science.1256297.
- Enserink, M., & Chin, G. (2015). The end of privacy. *Science*, 347(6221), 490–491. doi:10.1126/science.347.6221.490.
- Galaxhi, H., & Nah, F. F.-H. (2006). Privacy issues in the era of ubiquitous commerce. *Electronic Markets*, 16(3), 222–232. doi:10.1080/10196780600841894.
- Gogoulous, F. I., Antonakopoulou, A., Lioudakis, G. V., Mousas, A. S., & Kaklamani, D. I. (2014). On the design of a privacy aware authorization engine for collaborative environment. *Electronic Markets*, 24(2), 101–112. doi:10.1007/s12525-014-0155-9.
- Kieseberg, P., Schrittwieser, S., Mulazzani, M., Echizen, I., & Weippl, E. (2014). An algorithm for collusion-resistant anonymization and fingerprinting of sensitive microdata. *Electronic Markets*, 24(2), 113–124. doi:10.1007/s12525-014-0154-x.
- Kwok, S. H., Lui, S. M., Cheung, S. C., & Tam, K. Y. (2003). Digital rights management in web services. *Electronic Markets*, 13(2), 133–140. doi:10.1080/1019678032000067208.
- Liao, G.-Y., & Hwang, J.-J. (2001). A fair and privacy-preserved protocol for sealed-bid auctions. *Electronic Markets*, 11(3), 163–170. doi:10.1080/101967801681008004.
- Loebbecke, C. (2007). Piloting RFID along the supply chain: A case analysis. *Electronic Markets*, 17(1), 29–38. doi:10.1080/10196780601136773.
- Maguire, S., Friedberg, J., Nguyen, M.-H. C. & Haynes, P. (2015). A metadata-based architecture for user-centered data accountability. *Electronic Markets*, 25(2). doi:10.1007/s12525-015-0184-z.
- Mcknight, D. H., Kacmar, C. J., & Choudhury, V. (2004). Shifting factors and the ineffectiveness of third party assurance seals: a two-stage model of initial trust in a web business. *Electronic Markets*, 14(3), 252–266. doi:10.1080/1019678042000245263D.
- O'Reilly, P., Duane, A., & Andreev, P. (2012). To M-Pay or not to M-Pay - Realising the potential of smart phones: conceptual modeling and empirical validation. *Electronic Markets*, 22(4), 229–241. doi:10.1007/s12525-012-0105-3.
- Riquelme, I. P., & Román, S. (2014). Is the influence of privacy and security on online trust the same for all type of consumers? *Electronic Markets*, 24(2), 135–149. doi:10.1007/s12525-013-0145-3.
- Saeed, K. A., & Leitch, R. A. (2003). Controlling sourcing risk in electronic marketplaces. *Electronic Markets*, 13(2), 163–172. doi:10.1080/1019678032000067172.
- Spiekermann, S., Böhme, R., Acquisti, A. & Hui, K.-L. (2015a). Personal data markets. *Electronic Markets*, 25(2). doi:10.1007/s12525-015-0190-1.
- Spiekermann, S., Acquisti, A., Böhme, R. & Hui, K.-L. (2015b). The challenges of personal data markets and privacy. *Electronic Markets*, 25(2). doi:10.1007/s12525-015-0191-0.
- Strathoff, P. & Lutz, C. (2014). Privacy concerns and online behavior – Not so paradoxical after all? Viewing the privacy paradox through different theoretical lenses. In: S. Brändli, R. Schister & A. Tamò (Eds.), *Multinationale Unternehmen und Institutionen im Wandel – Herausforderungen für Wirtschaft, Recht und Gesellschaft*, (pp.81-99). Stämpfli Verlag. doi:10.2139/ssrn.2425132.
- Sun, Y., Liu, L., Peng, X., Dong, Y., & Barnes, S. J. (2014). Understanding Chinese users' continuance intention toward online social networks: an integrative theoretical model. *Electronic Markets*, 24(2), 57–66. doi:10.1007/s12525-013-0131-9.
- Sutanto, J., Palme, E., Tan, C.-H., & Phang, C. W. (2013). Addressing the personalization-privacy paradox: an empirical assessment from a field experiment on Smartphone users. *MIS Quarterly*, 37(4), 1141–1164.
- van Dycke, T. P., Midha, V., & Nemati, H. (2007). The effect of consumer privacy empowerment on trust and privacy concerns in E-commerce. *Electronic Markets*, 17(1), 68–81. doi:10.1080/10196780601136997.
- Wohlgemuth, S., Sackmann, S., Sonehara, N., & Tjoa, A. M. (2014). Security and privacy in business networking. *Electronic Markets*, 24(2), 81–88. doi:10.1007/s12525-014-0158-6.
- Xu, H., & Gupta, S. (2009). The effects of privacy concerns and personal innovativeness on potential and experienced customers' adoption of location-based services. *Electronic Markets*, 19(2/3), 137–149. doi:10.1007/s12525-009-0012-4.