



Editorial: Special issue on cyber security, privacy and ethics of information systems

Alessandro Acquisti¹ · Tamara Dinev² · Mark Keil³

Published online: 20 November 2019

© Springer Science+Business Media, LLC, part of Springer Nature 2019

This special Issue of Information Systems Frontiers, dedicated to the memory of H. Jeff Smith (Keil et al. 2019), contains a selection of manuscripts originally accepted for the ICIS 2018 track on Cyber Security, Privacy and Ethics of IS. Authors of all manuscripts accepted into the ICIS track were invited to submit revised versions of their manuscripts for peer-review at the journal. Six manuscripts were eventually chosen for this issue. The manuscripts encompass multiple methodologies (including meta-analysis, expert interviews, and experiments) and a plurality of topics (from information security compliance to the impact of data regulation on innovation; from identity theft to consumers' perceptions of information security). Together, they encapsulate and showcase the richness and variety of contemporary IS research at the intersection of security, privacy, trust, and ethics.

Three of the manuscripts focus on consumers' attitudes, behaviors, or reactions to privacy, security, and ethical issues in digital environments.

Ayaburi et al. (2019) present a study on individuals' self-regulation and habitual use of technology in unknown wireless networks use contexts. Their study asserts that regular use of wireless networks under deficient self-regulation (DSR) has created many negative outcomes, and few studies have explicated factors leading to such outcomes. To address this, the authors develop a conceptual self-regulation model that explains the antecedents and consequences of DSR and test the model using a survey instrument. Their findings suggest that DSR is a good predictor of individuals' habits (routine and automatic) of using technology in the wireless context. DSR increases the propensity to consciously or unconsciously connect to wireless networks habitually.

In a related work, Mohr and Walter (2019) shed light on how consumers form their perceptions of information security while buying goods online. Existing research has mainly focused on how information security concerns affect online behavior and online shopping. Using an Elaboration Likelihood model (ELM), the authors perform an exploratory and experimental study, dissecting the paradoxical security behavior and transfer of trust attitude that customers exhibit while shopping online. Their findings indicate that customers form their trusting beliefs towards a previously unknown retailer through the peripheral route of ELM based on technology or website sophistication, and that they transfer their trusting beliefs from the retailer to the trust expectation that their information will be secure.

Finally, Walsh et al. (2019) study consumers' fear of online identity theft (FOIT). Their study validates a previous scale (developed for the German context) in a cross-cultural setting, and also proposes an abbreviated version of the scale. The manuscript addresses two important issues. One is to better understand consumers' fear of online identity theft - a psychological barrier that can affect consumers' online decisions. A second issue is methodological: as cross-cultural analyses are of increasing importance in contemporary privacy and security research, the authors' efforts to test and increase the reliability, validity, and cross-national applicability of a measurement scale (namely, the FOIT scale) are of particular significance.

Three other manuscripts concentrate instead on firms' behavior, focusing on security compliance behavior, the security divide between SME and large companies, and the impact of privacy regulation on innovation.

Trang and Brendel (2019) examine the applicability of deterrence theory in information security policy compliance research. Their study echoes the concerns of information security managers in enforcing information security policy (ISP) in relation to both employee negligence and intentional insider breaches. The authors indicate the inconsistencies surrounding the support of deterrence theory for predicting ISP compliance behavior. The paper focuses on insiders'

✉ Alessandro Acquisti
acquisti@andrew.cmu.edu

¹ Carnegie Mellon University, Pittsburgh, PA 15213, USA

² Florida Atlantic University, Boca Raton, FL 33431, USA

³ Georgia State University, Atlanta, GA 30302, USA

compliance with information security policies and performs a meta-analysis of correlated literature on deterrence theory and ISP compliance behavior. Per the results of their analyses two aspects stand out. First, sanction severity and sanction certainty have significant influence while sanction celerity exhibits low effect on security compliance behavior. Secondly, in malicious contexts, cultures with a high degree of power distance, and cultures with a high uncertainty avoidance, deterrence theory is a suitable predictor of deviant behavior.

Heidt et al. (2019) investigate the security divide between SME and large companies. Given the significant relevance of SME for both the economy and society, the authors advocate that organizational IT security research needs to take the characteristics of SME into cognizance. The study proposes a framework that captures how internal SME-specific firm characteristics or external pressures and barriers affect their IT security investments. Based on 25 expert interviews and analyses of interview transcripts the authors find that limited resources, management style and personality of the managing director have profound effects on IT security decisions. The manuscript offers relevant discussions on trust-based relationships and the impactful role of affective and experiential factors in decision-making processes of potential customers.

Martin et al. (2019) embark on an analysis into the timely debate over the impact of privacy regulation on innovation. Against the backdrop of repeated claims that stricter regulation penalizes firms, the authors point out a relative lack of empirical evidence investigating the actual impact of data regulation on firms. Their study focuses on the introduction of the EU General Data Protection Regulation (GDPR). The authors use a multiple-stage semi-structured interviews approach (interviewing lawyers, senior managers in start-ups, and other intermediaries). Their findings paint a complex and nuanced picture: the authors identify and distill a set of likely responses of firms to GDPR, some of them positive and some negative from the standpoint of innovation. In essence, data regulation can simultaneously stimulate and constrain innovation.

We thank the various AEs (listed below) and referees who have given much of their time to comment on the papers and have shepherded the papers in this special issue towards publication. We also thank Angela Sasse, Ruhr University Bochum in Germany, who was a co-Track chair of the Cyber Security, Privacy and Ethics track for ICIS 2018 and who had to step out of the guest editor role for personal reasons. H. Raghav Rao, of the University of Texas at San Antonio, another co-Track chair at ICIS 2018 in San Francisco rendered invaluable help in bringing the special issue to fruition. Finally we thank Heng Xu of American University who was involved in this issue from the very start and was the igniting force behind it.

Guest Editors.

Alessandro Acquisti, Carnegie Mellon University; Tamara Dinev, Florida Atlantic University, Mark Keil, Georgia State University.

Associate Editors.

Idris Adjerid, Zinaida Benenson, Rainer Boehme, Ryan Calo, Teju Herath, Chris Hoofnagle, Gabriele Lenzini, Kichan Nam, Melanie Volkamer.

References

- Ayaburi E. W., Wairimu J., & Andoh-Baidoo F. K. (2019). Antecedents and outcome of deficient self-regulation in unknown wireless networks use context: An exploratory study. *Information Systems Frontiers*, 21(6). <https://doi.org/10.1007/s10796-019-09942-w>.
- Heidt M., Gerlach J. P., & Buxmann P. (2019). Investigating the security divide between SME and large companies: How SME characteristics influence organizational IT security investments. *Information Systems Frontiers*, 21(6). <https://doi.org/10.1007/s10796-019-09959-1>.
- Keil M., Culnan M., Dinev T., & Xu H. (2019). Data governance, consumer privacy, and project status reporting: Remembering H. Jeff Smith. *Information Systems Frontiers*, 21(6). <https://doi.org/10.1007/s10796-019-09964-4>.
- Martin N., Matt C., Niebel C., & Blind K. (2019). How data protection regulation affects startup innovation. *Information Systems Frontiers*, 21(6). <https://doi.org/10.1007/s10796-019-09960-8>.
- Mohr H., & Walter Z. (2019). Formation of consumers' perceived information security: Examining the transfer of Trust in Online Retailers. *Information Systems Frontiers*, 21(6). <https://doi.org/10.1007/s10796-019-09961-7>.
- Trang S., & Brendel B. (2019). A meta-analysis of deterrence theory in information security policy compliance research. *Information Systems Frontiers*, 21(6). <https://doi.org/10.1007/s10796-019-09956-4>.
- Walsh G., Shiu E., Hassan L., Hille P., & Takahashi I. (2019). Fear of online consumer identity theft: Cross-country application and short scale development. *Information Systems Frontiers*, 21(6). <https://doi.org/10.1007/s10796-019-09958-2>.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Dr. Alessandro Acquisti is a Professor of Information Technology and Public Policy at the Heinz College, Carnegie Mellon University (CMU), the PwC William W. Cooper Professor of Risk and Regulatory Innovation, and a Carnegie Fellow (inaugural class). He is the Director of the Peex (Privacy Economics Experiments) lab at CMU, and the Co-director of Carnegie Mellon's CBDR (Center for Behavioral and Decision Research). Dr. Acquisti investigates the economics of privacy. His studies have spearheaded the investigation of privacy and disclosure behavior in online social networks, and the application of behavioral economics to the study of privacy and information security decision making. His studies have won numerous awards and have been published in journals, books, and proceedings across different fields, including *Science*, *Proceedings of the National Academy of Science*, *Management Science*, *Journal of Economic Literature*, *Marketing Science*, *Journal of Consumer Research*, *Journal of Personality and Social Psychology*, and *Journal of Experimental Psychology*. Dr. Acquisti has testified before the U.S.

Senate and House committees on issues related to privacy policy and consumer behavior. His findings have been featured in national and international media outlets, including the Economist, the New York Times, the Wall Street Journal, the Washington Post, the Financial Times, [Wired.com](#), NPR, CNN, and 60 Minutes; his TED talks on privacy and human behavior have been viewed over 1.2 million times online. Dr. Acquisti holds a Ph.D. from UC Berkeley, and Master degrees from UC Berkeley, the London School of Economics, and Trinity College Dublin.

Dr. Tamara Dinev is Professor and Chair of the Department of Information Technology and Operations Management (ITOM), College of Business, Florida Atlantic University, Boca Raton, Florida. She received her Ph.D. in Theoretical Physics in 1997. Following several senior positions in information technology companies, her interests migrated to management information systems research, and in 2000 she joined the Florida Atlantic University ITOM faculty. Dr. Dinev is actively involved in research on information privacy, trust in online transactions and vendors, multicultural aspects of information technology usage and online behavior, and organizational and individual/employee behavior regarding computer and information security. She has published in premier and top journals, including *MIS Quarterly*, *Information Systems Research*, *Decision Sciences*, *Journal of the AIS*, *Journal of Strategic Information Systems*, *European Journal of Information Systems*, *Information Systems Journal*, *Communications of the ACM*, *International Journal of Electronic Commerce*, and others. She has received numerous best paper awards and nominations at major information system conferences. Dr. Dinev served as Senior Associate Editor of *European Journal of Information Systems* and *Guest Associate Editor of MISQ* on multiple occasions. She has also served multiple times as Track Chair and Associate Editor for the *International Conference of Information*

Systems (ICIS) and the *European Conference of Information Systems* (ECIS).

Dr. Mark Keil is a Regents' Professor of the University System of Georgia and the John B. Zellars Professor of Computer Information Systems at Georgia State University (GSU). He holds B.S.E., S.M., and D.B.A. degrees from Princeton University, M.I.T. Sloan School of Management, and Harvard Business School, respectively. At GSU, he has received Robinson College of Business Faculty Recognition Awards both for teaching and research, as well as the university's Alumni Distinguished Professor Award for outstanding achievements in scholarship, teaching, and service. In 2018, he received the PMI Research Achievement Award from the Project Management Institute and the AIS Fellow Award from the Association for Information Systems.

Dr. Keil's research focuses on IT project management and decision making and includes work on preventing IT project escalation, identifying and managing IT project risks, improving IT project status reporting, and IT implementation and use. He has published more than 100 refereed journal articles in such outlets as the *MIS Quarterly*, *Information Systems Research*, *Strategic Management Journal*, *Journal of Management Information Systems*, *Decision Sciences*, *IEEE Transactions on Engineering Management*, *Sloan Management Review*, and *California Management Review*. Dr. Keil currently serves as a Senior Editor for *MIS Quarterly* and is also on the editorial board of the *Journal of Management Information Systems*. He has also served as a Senior Editor for *Information Systems Research* and for the *Information Systems Journal*, Associate Editor for *MIS Quarterly* and *Information Systems Research*, Co-Editor-in-Chief of *The DATA BASE for Advances in Information Systems*, and as an editorial board member for *IEEE Transactions on Engineering Management*. Dr. Keil has also served as Division Chair for the Academy of Management's OCIS Division.