Data Privacy and Security in the Context of Corporate Digital Responsibility: A Scoping Review

K. Valerie Carl [1]

Abstract: The continuous digitalization affects private and professional lives alike, providing new chances but also threats for companies, consumers, and society. Particularly data privacy and security risks remain central for consumers. In this evolving setting, the concept of Corporate Digital Responsibility (CDR) gains traction. CDR provides a framework for the responsible application of digital technologies, thereby putting, inter alia, data privacy and security in a larger context. A remarkable amount of prior Information Systems (IS) research can be linked to facets of the concept of CDR. Hence, this study pursues the goal to evaluate the comprehensiveness of current research in IS, also guiding future research efforts. To address this goal, this study grounds on a scoping review to evaluate previous popularity in IS research. The results illustrate a need for a more comprehensive view on data privacy and security in the larger context of CDR in the IS discipline.

Keywords: Corporate Digital Responsibility, Information Systems, Scoping Review

1 Introduction

The ongoing digitalization allows for a plethora of digital products and services ranging from Big Data to more sophisticated Artificial Intelligence (AI) applications. These digital products share new chances for value creation but also condition new obstacles and threats [e.g., Sp22] in part due to the increasing amount of processed consumer data. In the course of the ongoing digitalization, central ethical and societal challenges concerning autonomy, balance of power, human dignity, justice, privacy, and security emerged [Ro18]. Consumers demand for more responsible and ethical corporate behavior, particularly concerning data privacy and security [e.g., Ma86, Mi21], thereby highly valuing, e.g., access and correction opportunities to personal data beyond legal requirements as well as an individualized information approach to data practices [Ca23]. Such activities bear the ability to influence consumers' perceptions of companies positively. Hence, research and practice account for that by developing rich insights into a comprehensive approach towards ethical corporate behavior. Within this evolving context, the concept of Corporate Digital Responsibility (CDR) gains traction. CDR provides guidance for companies on how to exploit the opportunities of digitalization while adequately addressing its risks by putting ethical implications of corporate behavior in the broader context of manifold corporate responsibilities. Above all, CDR provides a more comprehensive view on

[1] Goethe University Frankfurt/Main, Chair of Information Systems and Information Management, Theodor-W.-Adorno-Platz 4, D-60323 Frankfurt/Main, Germany, kcarl@wiwi.uni-frankfurt.de, https://orcid.org/0000-0003-4655-1046

corporate responsibilities in the digital context and allows a linked consideration and evaluation of the well-known, established individual sub-fields (e.g., data privacy and security). CDR applies to various kinds of digital technologies, products, and services despite their diverse characteristics and ethical requirements. The concept of CDR was highly practice-driven while now being an emerging topic in research [Lo21]. Yet, no research focused on providing a status-quo review of previous research on data privacy and security in the light of CDR, scoping the highly dispersed research field on corporate responsibilities in the digital context. Rather prior endeavors concentrated on summarizing research directly related to data privacy and security [e.g., SDX11]. To the best of knowledge, this study is the first to provide a scoping overview on existing research in IS that relates to the concept of CDR. This study evaluates the popularity and comprehensiveness of current research in the sense of the interlinked consideration of data privacy and security with various components of corporate responsibilities. Aiming to move data privacy and security forward in a broader context, the awareness where relatable research already resides is crucial. Hence, this study scopes previous, highly dispersed research efforts and links them to the new concept of CDR. Besides, this research provides guidance on future research paths in IS regarding data privacy and security in the light of CDR. Both contribute to the overarching aim of enabling a more comprehensive view on data privacy and security by establishing CDR in IS research. To achieve this, the next section introduces the concept of CDR and domain-specific sub-fields. Section three presents the methodology, while section four maps current research according to CDR sub-fields and provides a discussion on this study's results. Finally, this work concludes with the main insights and its limitations.

2 Corporate Digital Responsibility

CDR shares goals and closely relates to the concept of Corporate Social Responsibility (CSR). The concept of CDR especially accounts for the "exponential growth in technological development, malleability of technologies and data in use, and pervasiveness of technology and data" [Lo21, p.876], therefore requiring the consideration as a separate concept, since these particularities are not explicitly covered by CSR [Mih22]. CDR gains increasing traction in research and a consensus of the concept understanding emerges [Mih22]. Many different approaches to CDR developed with differing nomenclature and foci, sharing a common understanding [Mih22, Mu22]. This study employs an approach consisting of eight sub-fields [Th17] developed in the current CDR debate (see Table 1). Some of the sub-fields are subject to regulations (e.g., the GDPR). However, CDR describes the voluntary assumption of responsibilities beyond the legal minimum.

CDR sub-field	Sub-field description
Data privacy and security	The protection of consumers' data privacy and security should be ensured (e.g., restricted data usage).

Education and awareness	Consumers should be educated, including raised awareness of ecological, social, societal, and economic consequences of their consumption (e.g., resource consumption in usage).
Information and transparency	Consumers should have access to appropriate information adapted to their individual needs (e.g., product information).
Economic interests	The economic interests of consumers should be protected and promoted (e.g., through the deployed business model).
Product safety and liability	Consumers should be protected from risks to their health and safety (e.g., their mental safety especially in social media).
Access	Consumers should have access to basic digital products and services: mentally and physically (e.g., access to software).
Dispute resolution and awareness	Consumers should have access to effective dispute settlement and redress procedures (e.g., complaint handling).
Governance and participation mechanisms	Companies should provide appropriate participation mechanisms for interested parties (e.g., in the product development).

Tab. 1: Overview of CDR sub-fields [following Th17, adapted from Mi21]

The individual CDR sub-fields are not new to IS research. CDR puts the manifold corporate responsibilities in a broader, interconnected context to provide a more holistic approach to corporate responsibilities. Especially in practice, corporate responsibilities are interwoven and do not appear isolated but activities related to one sub-field can have a cross-effect. The concept of CDR ensures the integrated evaluation of corporate responsibilities (e.g., data privacy and security) across different subfields, thereby better reflecting reality. The concept applies to various stakeholder groups (e.g., employees, consumers) [e.g., Lo21]. To ensure a solid research approach, this study focuses on CDR commitment directed at consumers as one key stakeholder group.

3 Allgemeine Formatierung

Scoping reviews, also called mapping studies, approach current research on a distinct topic. They share the same basic methodology with systematic literature reviews [KBP11]. Albeit, they differ in their designated goal. Systematic literature reviews aim at aggregating research results in detail, whereas scoping reviews should provide an overview and classification of previous research activities to serve as an initial orientation for other researchers [e.g., KBP11], e.g., concerning popularity. Besides, scoping reviews aim at identifying areas with a need for additional research [e.g., KBP11], thus guiding towards future research paths. Scoping reviews are increasingly used in IS research to give an overview of scattered research and to motivate future research on emerging topics [e.g., Li18].

Conducting the scoping review, this study follows the aggregated guidelines by Petersen

and colleagues [PVK15] to provide a systematic and transparent process also ensuring rigor, reliability, and trustable results. During the whole conceptualization, actual search, and evaluation phase a detailed review protocol keeps record of the process and corresponding decisions. The keyword selection grounds on the aim of CDR: ethical and responsible behavior of companies in the digital context. To determine appropriate keywords, we drew on prior knowledge, yearlong experience with the topic, and an initial unstructured analysis. The concept-related keywords form one set of keywords and aim to cover ethical behavior (i.e., (("corporate" OR "business") AND "responsibility") OR "ethic*"). In this vein, we opted against searching for the respective eight sub-fields derived from the CDR debate not to limit the search to these eight fields, rather searching more openly. Besides, this study employs an object-related keyword set to narrow the results to the relevant digital context (i.e., "product" OR "good" OR "service" OR "tech*" OR "econ*" OR "platform*" OR "market" OR "commerce"). This study uses wildcards and Boolean operators. The search term consists of the domain keyword sets linked with "AND" searching title, classification codes, abstract, keyword, and subjects.

This scoping review focuses on prior publications in IS research to provide guidance on data privacy and security research in the light of CDR within this specific research domain. This study incorporates only the eight top-ranked IS journals, the Senior Scholars' Basket Journals, focusing on IS outlets and ensuring a high reputation for quality. The search process covers every journal independently using the same search criteria. The exclusion of publications in other disciplines like computer science is due to the goal of the publication to stimulate and guide research in IS. The search should provide a picture as up-to-date as possible, thus conducted in autumn 2022 incorporating publications of the first half year. In total, the search yields 224 publications. Two researchers independently performed each step of the scoping review process, discussed their results after each step, and formed consensus on the final assessment. The search process includes the initial screening of the derived publications according to their title, abstract, and keywords. One criteria of exclusion applies to publications that are not adaptable to or focus on corporate responsibilities in the digital context. Still, this study includes research not designated to CDR due to the concept's novelty. Additionally, the final set of publications only consists of research with a business-to-consumer focus compared to a business-to-business one. Summing up, the initial evaluation leads to the exclusion of 107 publications due to the misfit with the aforementioned exclusion criteria. Thus, the second step of the review process features 117 publications for a detailed analysis of the articles' full texts according to the same exclusion criteria, leading to the exclusion of another 71 publications. Hence, the third step of the scoping review includes 46 articles and aims at coding them according to acknowledged practices. Yet, there is no suiting coding scheme available for CDR sub-fields. For the development of a suiting coding scheme, this study employs the nomenclature of the eight sub-fields of CDR [Th17]. The scheme is a multiple classification scheme (i.e., coders can classify publications into more than one sub-field). This classification approach serves as an orientation framework and therefore should lead to a discursive and iterative process. Both coders performed coding independently first, discussed their results and deviations in coding, and solved them in mutual agreement

following established procedures in IS research [e.g., Li18], thereby developing a codebook and applying it to the sample in a second coding round based on the same nomenclature but with a broader understanding of each of the eight sub-fields.

4 Data Privacy and security in the context of CDR

The aim of this study is to scope prior research relatable to the concept of CDR and therefore to enable a more comprehensive view on data privacy and security in IS research. The results of the conducted scoping review indicate a growing interest in CDR-relatable research (see Table 2). While in the early years only a few publications addressed responsibilities in the digital context, research interest since 2007 has been at a comparatively higher level (except for 2013 and 2014). Particularly in 2021, research interest in responsibilities in the digital context has been extremely high. The results highlight the timeliness of research in this area, thereby motivating continued research concerning a comprehensive approach to corporate responsibilities (e.g., data privacy and security) in future.

		Data privacy & security	Education & awareness	Information & transparency	Economic interests	Product safety & liability	Access	Dispute resolution & awareness	Governance & participation mechanisms
1986	[Ma86]	**x**					x		
1992	[Oz92]	**x**	x		x				
1993	[Cu93]	**x**							
1994	[BO94]		x						x
	[MK94]		x				x		
	[WT94]								x
1997	[CS97]			x					
2000	[AW00]								x
2001	[VB01]						x		
2002	[SS02]	**x**							
	[SSN02]			x				x	
2003	[HM03]						x		
2007	[CD07]							x	
	[Cl07]			x					

	[OD07]		x				x		x
	[PW07]				x				
	[St07]	**x**					x		
2008	[SK08]	**x**		x			x	x	
	[THS08]	**x**		x				x	
	[TYC08]							x	
2009	[LSL09]	**x**		x		x	x		
2010	[MW10]	**x**		x			x		
	[WBC10]		x	x	x				
2011	[SDX11]	**x**							
	[XB11]	**x**	x	x	x				
2012	[SDS12]	**x**		x					
	[St12]	**x**							
	[Te12]	**x**		x	x				
2015	[GCC15]	**x**	x	x					
	[Hu15]								x
2016	[Ra16]	**x**			x	x	x		
	[XXL16]			x		x			
2017	[ABK17]	**x**		x	x				
2018	[SRK18]					x			
2019	[Ch19]	**x**		x					
2020	[WSM20]	**x**		x	x				
2021	[Be21]	**x**		x	x	x			
	[DJR21]					x		x	
	[DT21]	**x**					x		
	[MNH21]			x					
	[MVL21]	**x**			x		x		
	[NPN21]	**x**		x	x	x			x
	[SM21]	**x**			x	x			
	[Wo21]			x		x			
2022	[KG22]			x	x				

[Mik22]	**x**		x	x	x			

Tab. 2: Classification of the scoped publications according to CDR sub-fields covered

When assessing research interest on sub-field-level, our findings indicate that (isolated) research on data privacy and security is well established. This sub-field is most dominantly researched in this study (see Table 2). Research interest was stable throughout the whole study period. In the recent years, however, research on the topic intensified.

Despite the high importance of data privacy and security for companies and consumers alike [e.g., Ca23], future research should go beyond an isolated approach to this sub-field. Table 2 indicates that research on data privacy and security in the light of the overarching concept CDR is not yet comprehensive. While comparably many publications address data privacy and security simultaneously with sub-fields like information and transparency or access [e.g., Ch19, DT21], only few publications address data privacy and security and dispute resolution and awareness or education and awareness [e.g., GCC15, THS08] in parallel. These results indicate a lacking interconnected understanding of data privacy and security with further sub-fields, particularly since dispute resolution and awareness and education and awareness have a strong applicability in the context of data privacy and security. Hence, future research should develop an enhanced understanding of these CDR sub-fields and their influences on one another.

Above all, the total coverage in Table 2 indicates that only relatively few publications adopt a broader view of corporate responsibilities across different issues [e.g., NPN21, Ra16] and none the whole concept spectrum, thereby not discussing data privacy and security in the broadest possible context. IS research on CDR-related topics is more isolated and reveals a more dispersed research field, implying the danger of disconnected research. Albeit recent IS publications follow a broader approach to digital responsibility with more sub-fields covered (on average) in parallel per publication. This emphasizes the broadening approach to digital responsibility, underpinning the usefulness of a concept such as CDR, which places individual digital responsibility areas such as data privacy and security in the broader context and thus enables a more comprehensive approach to them. Future research should adopt this broader perspective. In this way, a realistic understanding of the interwoven and influencing responsibilities can be developed. This helps researchers to understand these interrelationships better, but also supports practitioners in the implementation. In this way, the understanding of corporate responsibilities concerning data privacy and security can evolve, particularly becoming more comprehensive.

5 Conclusion

This research provides an initial systematic overview on previous highly dispersed research efforts in leading IS outlets. Aim of this study is to assess the popularity of data privacy and security in the light of the umbrella concept CDR in IS research. This study's

results corroborate that research on corporate responsibilities in the digital context, particularly data privacy and security, is well established in IS research. Rather, research remains incoherent and disconnected. Ultimately, this study sheds light on future research paths worth considering in IS research. None of the evaluated publications addresses the full range of CDR sub-fields simultaneously. However, corporate responsibilities never occur in isolation in practice. Hence, a holistic approach to data privacy and security, e.g., employing CDR, can help to understand the extent of corporate responsibilities and the influences of the sub-fields on another. Summing up, this study theoretically contributes to the existing knowledge on data privacy and security as well as CDR in IS research. The scoping of the examined publications contributes to a better understanding of the status-quo of research relatable to CDR and its distinctive sub-fields focusing on data privacy and security research. Additionally, this study's results motivate and inform IS researchers concerning future research paths in the context of data privacy and security employing a comprehensive approach such as CDR.

Despite best efforts, some limitations apply. Firstly, this study is not and was not meant to be exhaustive. There is a deliberate focus on IS research. Secondly, this study focuses on CDR activities geared to consumers. Still, CDR provides a broad field of action applicable to, e.g., employees, business-to-business activities, or society itself. Future research should incorporate these differing stakeholder groups and their respective viewpoints.

To this end, goal of this publication is to motivate future work on data privacy and security in the context of CDR. This will shed light on yet underexplored research areas but also stimulate the discovery of novel fields worth considering.

Acknowledgement

The Hessian State Chancellery – Hessian Minister of Digital Strategy and Development supported this work under the promotional reference 6/493/71574093 (CDR-CAT).

Bibliography

[ABK17] Anderson, C.; Baskerville, R. L.; Kaul, M.: Information Security Control Theory: Achieving a Sustainable Reconciliation Between Sharing and Protecting the Privacy of Information. Journal of Management Information Systems 34/4, pp. 1082-1112, 2017.

[AW00] Adman, P.; Warren, L.: Participatory Sociotechnical Design of Organizations and Information Systems – An Adaptation of Ethics Methodology. Journal of Information Technology 15/1, pp. 39-51, 2000.

[Be21] Berente, N. et al.: Managing Artificial Intelligence. MIS Quarterly 45/3, pp. 1433-1450, 2021.

[BO94] Beath, C. M.; Orlikowski, W. J.: The Contradictory Structure of Systems Development Methodologies: Deconstructing the IS-User Relationship in Information Engineering. Information Systems Research 5/4, pp. 350-377, 1994.

[Ca23] Carl, K. V. et al.: Consumer Perspective on Corporate Digital Responsibility—An Empirical Evaluation of Consumer Preferences. Journal of Business Economics, Forthcoming, 2023.

[CD07] Costello, G. J.; Donnellan, B.: The Diffusion of WOZ: Expanding the Topology of IS Innovations. Journal of Information Technology 22/1, pp. 79-86, 2007.

[Ch19] Chanson, M. et al.: Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data. Journal of the Association for Information Systems 20/9, pp. 1274-1309, 2019.

[Cl07] Clemons, E. K.: An Empirical Investigation of Third-Party Seller Rating Systems in E-Commerce: The Case of buySAFE. Journal of Management Information Systems 24/2, pp. 43-71, 2007.

[CS97] Choudhury, V.; Sampler, J. L.: Information Specificity and Environmental Scanning: An Economic Perspective. MIS Quarterly 21/1, pp. 25-53, 1997.

[Cu93] Culnan, M. J.: "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. MIS Quarterly 17/3, pp. 341-363, 1993.

[DJR21] Dunn, B.; Jensen, M. L.; Ralston, R.: Attribution of Responsibility After Failures Within Platform Ecosystems. Journal of Management Information Systems 38/2, pp. 546-570, 2021.

[DT21] Díaz Andrade, A.; Techatassanasoontorn, A. A.: Digital Enforcement: Rethinking the Pursuit of a Digitally-Enabled Society. Information Systems Journal 31/1, pp. 184-197, 2021.

[GCC15] Greenaway, K. E.; Chan, Y. E.; Crossler, R. E.: Company Information Privacy Orientation: A Conceptual Framework. Information Systems Journal 25/6, pp. 579-606, 2015.

[HM03] Heng, M. S. H.; de Moor, A.: From Habermas's Communicative Theory to Practice on the Internet. Information Systems Journal 13/4, pp. 331-352, 2003.

[Hu15] Hutter, K. et al.: Machiavellianism or Morality: Which Behavior Pays Off in Online Innovation Contests? Journal of Management Information Systems 32/3, pp. 197-228, 2015.

[KBP11] Kitchenham, B. A.; Budgen, D.; Pearl Brereton, O.: Using Mapping Studies as the Basis for Further Research – A Participant-Observer Case Study. Information and Software Technology 53/6, pp. 638-651, 2011.

[KG22] Kordzadeh, N.; Ghasemaghaei, M.: Algorithmic Bias: Review, Synthesis, and Future Research Directions. European Journal of Information Systems 31/3, pp. 388-409, 2022.

[Li18] Li, Y. et al.: Blockchain Technology in Business Organizations: A Scoping Review. In: Proceedings of the 51st Hawaii International Conference on System Sciences (HICCS), pp. 4474-4483, 2018.

[Lo21] Lobschat, L. et al.: Corporate Digital Responsibility. Journal of Business Research 122, pp. 875-888, 2021.

[LSL09] Lee, S.; Shin, B.; Lee, H. G.: Understanding Post-Adoption Usage of Mobile Data Services: The Role of Supplier-Side Variables. Journal of the Association for Information Systems 10/12, pp. 860-888, 2009.

[Ma86] Mason, R. O.: Four Ethical Issues of the Information Age. MIS Quarterly 10/1, pp. 5-12, 1986.

[Mi21] Mihale-Wilson, C. et al.: Corporate Digital Responsibility – Extended Conceptualization and a Guide to Implementation. In: Proceedings of the European Conference on Information Systems (ECIS), 2021.

[Mih22] Mihale-Wilson, C. et al.: Corporate Digital Responsibility: Relevance and Opportunities for Business and Information Systems Engineering. Business & Information Systems Engineering 64/2, pp. 127-132, 2022.

[Mik22] Mikalef, P. et al.: Thinking Responsibly About Responsible AI and "the Dark Side" of AI. European Journal of Information Systems 31/3, pp. 257-268, 2022.

[MK94] Mirani, R.; King, W. R.: Impacts of End-User and Information Center Characteristics on End-User Computing Support. Journal of Management Information Systems 11/1, pp. 141-166, 1994.

[MNH21] Marabelli, M.; Newell, S.; Handunge, V.: The Lifecycle of Algorithmic Decision-Making Systems: Organizational Choices and Ethical Challenges. Journal of Strategic Information Systems 30/3, pp. 1-15, 2021.

[Mu22] Mueller, B.: Corporate Digital Responsibility. Business & Information Systems Engineering 64, pp. 689-700, 2022.

[MVL21] Marabelli, M.; Vaast, E.; Li, J. L.: Preventing the Digital Scars of COVID-19. European

Journal of Information Systems 30/2, pp. 176-192, 2021.

[MW10] Mingers, J.; Walsham, G.: Toward Ethical Information Systems: The Contribution of Discourse Ethics. MIS Quarterly 34/4, pp. 833-854, 2010.

[NPN21] Nussbaumer, A.; Pope, A.; Neville, K.: A Framework for Applying Ethics-by-Design to Decision Support Systems for Emergency Management. Information Systems Journal 33/1, pp. 34-55, 2021.

[OD07] Olphert, W.; Damodaran, L.: Citizen Participation and Engagement in the Design of E-Government Services: The Missing Link in Effective ICT Design and Delivery. Journal of the Association for Information Systems 8/9, pp. 491-507, 2007.

[Oz92] Oz, E.: Ethical Standards for Information Systems Professionals: A Case for a Unified Code. MIS Quarterly 16/4, pp. 423-433, 1992.

[PVK15] Petersen, K.; Vakkalanka, S.; Kuzniarz, L.: Guidelines for Conducting Systematic Mapping Studies in Software Engineering: An Update. Information and Software Technology 64, pp. 1-18, 2015.

[PW07] Parameswaran, M.; Whinston, A.: Research Issues in Social Computing. Journal of the Association for Information Systems 8/6, pp. 336-350, 2007.

[Ra16] Ransbotham, S. et al.: Special Section Introduction—Ubiquitous IT and Digital Vulnerabilities. Information Systems Research 27/4, pp. 834-847, 2016.

[Ro18] Royakkers, L. et al.: Societal and Ethical Issues of Digitization. Ethics and Information Technology 20/2, pp. 127-142, 2018.

[SDS12] Stahl, B. C.; Doherty, N. F.; Shaw, M.: Information Security Policies in the UK Healthcare Sector: A Critical Evaluation. Information Systems Journal 22/1, pp. 77-94, 2012.

[SDX11] Smith, H. J.; Dinev, T.; Xu, H.: Information Privacy Research: An Interdisciplinary Review. MIS Quarterly 35/4, pp. 989-1015, 2011.

[SK08] Son, J.-Y.; Kim, S. S.: Internet Users' Information Privacy-Protective Responses: A Taxonomy and a Nomological Model. MIS Quarterly 32/3, pp. 503-529, 2008.

[SM21] Stahl, B. C.; Markus, M. L.: Let's Claim the Authority to Speak Out on the Ethics of Smart Information Systems. MIS Quarterly 45/1, pp. 485-488, 2021.

[Sp22] Spiekermann, S. et al.: Values and Ethics in Information Systems. Business & Information Systems Engineering 64, pp. 247-264, 2022.

[SRK18] Seymour, M.; Riemer, K.; Kay, J.: Actors, Avatars and Agents: Potentials and Implications of Natural Face Technology for the Creation of Realistic Visual Presence. Journal of the Association for Information Systems 19/10, pp. 953-981, 2018.

[SS02] Stewart, K. A.; Segars, A. H.: An Empirical Examination of the Concern for Information Privacy Instrument. Information Systems Research 13/1, pp. 36-49, 2002.

[SSN02] Shim, J. P.; Shin, Y. B.; Nottingham, L.: Retailer Web Site Influence on Customer Shopping: Exploratory Study on Key Factors of Customer Satisfaction. Journal of the Association for Information Systems 3/1, pp. 53-76, 2002.

[St07] Stahl, B. C.: ETHICS, Morality and Critique: An Essay on Enid Mumford's Socio-Technical Approach. Journal of the Association for Information Systems 8/9, pp. 479-490, 2007.

[St12] Stahl, B. C.: Morality, Ethics, and Reflection: A Categorization of Normative IS Research. Journal of the Association for Information Systems 13/8, pp. 636-656, 2012.

[Te12] Temizkan, O. et al.: Patch Release Behaviors of Software Vendors in Response to Vulnerabilities: An Empirical Analysis. Journal of Management Information Systems 28/4, pp. 305-338, 2012.

[Th17] Thorun, C. et al.: Indicators of Consumer Protection and Empowerment in the Digital World. Results and Recommendations of a Feasibility Study. https://www.conpolicy.de/data/user_upload/Studien/ConPolicy_Indicator_study.pdf, 2017.

[THS08] Tang, Z.; Hu, Y.; Smith, M. D.: Gaining Trust through Online Privacy Protection: Self-Regulation, Mandatory Standards, or Caveat Emptor. Journal of Management Information Systems 24/4, pp. 153-173, 2008.

[TYC08] Turel, O.; Yuan, Y.; Connelly, C. E.: In Justice We Trust: Predicting User Acceptance of E-Customer Services. Journal of Management Information Systems 24/4, pp. 123-151, 2008.

[VB01] Venkatesh, V.; Brown, S. A.: A Longitudinal Investigation of Personal Computers in Homes: Adoption Determinants and Emerging Challenges. MIS Quarterly 25/1, p. 71-102, 2001.

[WBC10] Watson, R. T.; Boudreau, M.-C.; Chen, A. J.: Information Systems and Environmentally Sustainable Development: Energy Informatics and New Directions for the IS Community. MIS Quarterly 34/1, pp. 23-38, 2010.

[Wo21] Wong, R. Y. M. et al.: Standing Up or Standing By: Understanding Bystanders' Proactive Reporting Responses to Social Media Harassment. Information Systems

Research 32/2, pp. 561-581, 2021.

[WSM20] Wiener, M.; Saunders, C.; Marabelli, M.: Big-Data Business Models: A Critical Literature Review and Multiperspective Research Framework. Journal of Information Technology 35/1, pp. 66-91, 2020.

[WT94] Wong, E. Y. W.; Tate, G.: A Study of User Participation in Information Systems Development. Journal of Information Technology 9/1, pp. 51-60, 1994.

[XB11] Xiao, B.; Benbasat, I.: Product-Related Deception in E-Commerce: A Theoretical Perspective. MIS Quarterly 35/1, pp. 169-196, 2011.

[XXL16] Xu, B.; Xu, Z.; Li, D.: Internet Aggression in Online Communities: A Contemporary Deterrence Perspective. Information Systems Journal 26/6, pp. 641-667, 2016.