Corporate Digital Responsibility: Evaluating Privacy and Data Security Activities on Company-level

K. Valerie Carl[1]

Abstract: The digital economy holds new opportunities for value creation but also threats for both companies and customers. Within this setting, the concept of Corporate Digital Responsibility (CDR) gains traction. Building on the well-established concept of Corporate Social Responsibility, CDR entails a set of principles through which it seeks to ensure an ethical and responsible development, deployment, and use of digital technologies. To date, the scholarly conceptualization of CDR is still in its infancy. This study pursues two main objectives: Firstly, it seeks to contribute to CDR theory by providing a more in-depth conceptualization with focus on privacy and data security. Secondly, this study provides first guidance for the evaluation of CDR activities on company-level, a benchmark corpus. As work-in-progress, the focus lies on identifying a starting point for the evaluation of CDR activities concentrating on privacy and data security, and hence research opportunities related to this assessment in future.

Keywords: corporate digital responsibility, ethical guidelines, data privacy, data security, benchmark corpus

1 Introduction

Advancements in digital technologies allow for the development of more sophisticated digital products and services. Especially, a plethora of Big Data and Artificial Intelligence applications emerged, further referred to under the umbrella term digital products and services. Nevertheless, besides all the new opportunities for value creation, digitalization also holds a range of threats and challenges [He16], [Th17], that managers need to cope with. Especially the collection of user data are accompanied by possible hazard of privacy and security related issues, sometimes causing economic, ethical, or legal issues for customers and firms alike [Ba19]. In an attempt to harness the advantages of digitization by adequately addressing its challenges, the emergence of a more comprehensive concept called Corporate Digital Responsibility (CDR) can be observed.

At its core, CDR is closely related to and has similar goals like the concept of Corporate Social Responsibility (CSR). While CSR aims to minimize the negative impacts and maximize the positive outcomes of corporate practices on socially and environmentally relevant issues [MR02], CDR intends to minimize the adverse effects of digitization while maximizing the positive impacts of corporate digital activities. In this vein, CDR seeks to

[1] Goethe University Frankfurt, Chair of Information Systems and Information Management, Theodor-W.-Adorno-Platz 4, 60323, Frankfurt am Main, kcarl@wiwi.uni-frankfurt.de

ensure an ethical and responsible development, deployment, and use of digital technologies and data. CDR puts, inter alia, privacy and data security attempts in a broader context to provide a more holistic approach.

To date, the CDR debate is strongly driven by practitioners and other policy-related initiatives, as its scholarly conceptualization is still in its infancy [Lo21] albeit digitization already brought up unprecedented challenges [Na17]. Recently, numerous initiatives evolved around the concept of CDR or widened their focus concerning this subject. Supranational organizations like the European Union, the OECD, or the UN are developing guidelines, laws (e.g., 'European General Data Protection Regulation' (GDPR), 'European Business Network for Corporate Social Responsibility', 'OECD Guidelines for Multinational Enterprises', 'UN Sustainable Development Goals', 'UN Global Compact'), or working groups which try to establish CDR in the corporate mind-set. Also, national and industry-led initiatives (e.g., the German 'Corporate Digital Responsibility Initiative') form up, where industry leaders want to set a good example by committing to ethical business practices in the digital world. Within this debate, experts have formulated eight CDR norms as a basis for ethical and responsible digital business practices [Th17].

Aiming to advance the scholarly debate on CDR, this study pursues two main objectives: Firstly, as a theoretical contribution, this study seeks to contribute to the emerging knowledge about CDR. An approach covering a total of 8 dimensions has already been devised [Th17]. To this end, this work theoretically links the concept of privacy and data security to the broader context of corporate responsibility, motivating research on CDR, and privacy and data security attempts as a distinct topic. Secondly, there are currently no concrete recommendations on how to evaluate CDR activities on company-level. This work seeks to close this theoretical gap, while at the same time contributing to the implementation of CDR in practice by providing a benchmark corpus. The implementation of CDR norms and practices can be pursued in many ways and at various levels [MM08]. This allows the company to position in relation to competitors and thus gain competitive advantages. As resources to be spent on CSR and CDR are limited, a successful CDR implementation hinges on companies' ability to evaluate activities regarding CDR norms.

This paper theorizes exemplary measures to evaluate CDR activities of a firm on the example of privacy and data security serving as an evaluation guideline. As work-in-progress, the focus lies on identifying new research opportunities related to the field of CDR with particular emphasis on privacy and data security to evaluate corporate activities. This research is based on previous research, own CDR surveys, and observations in practice.

2 Corporate Digital Responsibility

As mentioned previously, the Corporate Digital Responsibility (CDR) concept is closely related to the concept of Corporate Social Responsibility (CSR). Nevertheless, CDR merits scholarly attention on its own, as it accommodates the digital world's peculiar challenges [Lo21]. By drawing on existing literature regarding the unique ethical and social

challenges, that the digital context presents, this work discusses CDR's core components with a focus on privacy and data security. This will lay the foundation for evaluating CDR activities on the company-level.

Although CSR and CDR share common values, norms, and an organization's commitment towards ecological and social challenges at large, CDR should be considered separately from CSR. CDR addresses challenges to organizations' ethical behavior that are unique to the digital world and go far beyond CSR. Especially, "exponential growth in technological development, malleability of technologies and data in use, and pervasiveness of technology and data" [Lo21, p. 876] manifest particularities of digital technologies. Thus, CDR and CSR represent complementary but also sometimes overlapping concepts of business ethics. Compared to CSR, CDR addresses the unprecedented challenges related to the digital world. An approach comprising of a total of 8 dimensions to cover possible CDR activities has already been devised [Th17]. Table 1 presents these CDR norms proposed by practice and indicates exemplary related literature.

CDR norm [Th17]	**Norm description** [based on Th17]	**Related work**
I. Access	Consumers should have access to basic digital goods and services.	[HRK08]; [LMH17]; [VS13]
II. Education and awareness	Consumers should be educated including their awareness of ecological, social, societal, and economic aspects of their consumption.	
III. Information and transparency	Consumers should have access to appropriate information so that they can be informed according to their individual wishes and needs.	[AK06]; [GGK10]
IV. Economic interests	The economic interests of consumers should be protected and promoted.	[BKV15]; [HHS11]
V. Product safety and liability	Consumers should be protected from risks to their health and safety.	[DR95]; [Sm17]
VI. Privacy and data security	The protection of consumers' privacy, the free flow of information, and protected and secure payment mechanisms should be ensured.	[BC11]; [Gi18]; [Oe17]
VII. Dispute resolution and awareness	Consumers should have access to effective dispute settlement and appeal procedures.	[Eu16]; [Th17]
VIII. Governance and participation mechanisms	Legal organizations and regulators should ensure that there are appropriate governance and participation mechanisms in place.	[Lo21]; [Th17]

Tab. 1: CDR norms that can serve as a preliminary conceptualization and exemplary related work.

As resources to be spent on CSR and CDR are limited, a successful CDR implementation hinges on companies' ability to evaluate CDR norms and measures. Due to the complexity of building a benchmark corpus covering all dimensions of CDR, a first focus is placed on the applications that are most important for key stakeholders involved [KBM13]. According to previous research, the dimension of privacy and data security has been evaluated

most important from the customers' perspective [Mi21]. Hence, the development of a benchmark corpus to evaluate CDR activities on company-level firstly concentrates on the dimension of privacy and data security, while also taking into consideration possible overlaps with further CDR dimensions.

3 Evaluating CDR activities regarding privacy and data security

3.1 Evaluating activities within the privacy and data security norm

While data privacy focuses on consumers' capability to exert control over the storing, processing, or forwarding practices concerning their data, information security refers to the protection of stored data against various threats [BC11]. To date, privacy and data security remain two of the significant concerns related to the adoption and use of information technologies [Ma86], [MZH17]. Hence, the importance of data privacy and security is a widely discussed research topic in information systems (e.g., [BC11], [Ha02], [HH18]). Amongst one of the undisputed major consumer concerns in the digital economy, information privacy refers, inter alia, to the consumers' capability to control their information stored and the handling of their data, including the monetization [BC11], [Go91], [We67]. The topic is subject to regulations (e.g., GDPR), which define the minimum requirements of privacy and data security companies must comply with. While non-compliance with the minimum requirements can have negative legal and financial consequences [GS09], [Oe17], compliance often does not stand out positively. Against the background that companies can positively influence consumers' perceptions through strategic initiatives [Ha07], the CDR norm regarding privacy and data security encourages companies to outperform the current (legal) regulations.

The topic of privacy and data security is multifaceted and features various aspects. Smith et al. [SMB96], for instance, suggest that privacy has four main aspects: the first aspect of privacy relates to data collection. The second aspect adheres to unauthorized secondary use of information for both organization-specific internal and other external purposes. Further, the third privacy aspect is improper access, while information accuracy (i.e., errors) represents the fourth important privacy aspect. In practice, these aspects reappear in data privacy and security regulations such as the GDPR or OECD Privacy Framework. According to the OECD [Oe13] guidelines, for instance, privacy and data security should consider eight main principles: (1) data collection limitation; (2) data quality; (3) purpose specification; (4) use limitation; (5) security safeguards; (6) openness; (7) individual participation; (8) accountability principle. Akin, the GDPR provides eleven privacy and security-relevant principles [Te18], similar to the OECD Guidelines. The selected subdimensions cover seven of the eight main principles within the OECD Privacy Framework. The principle of accountability was excluded as it can be seen as a framework condition for the appropriate fulfillment of the other principles. Nevertheless, the use of such a data controller, as part of the accountability principle, is of crucial importance and should not be neglected by companies. Based on scholarly work on data privacy and security, and the

current state of legislation (i.e., GDPR, OECD Guidelines), a theory link to seven exemplary implementation measures of the data privacy and security CDR norm was drawn (see Table 2).

To evaluate privacy and data security activities on company-level a measurement scale has to be developed. Each sub-dimension of a CDR norm represents a broad field of application, thus, one subordinate possible measure was chosen to exemplarily discuss the evaluation of privacy and data security activities on company-level. Each measure features three different levels to apply an ample-based approach to evaluate CDR activities of companies. The first level is used to illustrate minimal activities related to the CDR implementation and partly coincides with the (national) statutory requirements for companies. Accordingly, CDR activities below the minimal activities would not be counted as corporate activities related to CDR. Still, CDR is a concept based on voluntariness, accordingly no company has to meet such levels. The further levels represent increasing, voluntary acceptance of more responsibility with regard to CDR. In that way, the evaluation of privacy and data security activities on company-level can be performed by applying this ample-based approach to differentiate between minimal activities to prominent takeover of additional responsibility (see Table 2).

Limited or restricted data collection must be with the consent of the user. Nevertheless, many consumers struggle to understand what data companies are really collecting, thus making uninformed decisions [Wi21]. Even though companies have to inform about this in an understandable way according to the GDPR [Fe19]. Thus the measure information regarding data protection has been included to cover the aforementioned sub-dimension exemplarily.

In line with this, the **clear purpose of data collection** is often communicated in a way that is difficult to understand [Di13]. Still, the purpose of the data collection should be clearly stated at the time of collection avoiding contradictions between the threefold communication to the customer and the actual declaration, for example, in the data protection declaration. Additionally, consumers might not be aware of the general agreement on the acceptance of the data protection declaration at the time of providing additional data to a firm. Following, the communication of the purpose at the time of data collection is essential for a responsible handling of user data and therefore exemplarily incorporated in the benchmark corpus.

In the same vein, **restricted data use** should be established to avoid unknown or unintended secondary usage, especially when it comes to third-party access [Di13]. On the one hand, firms might not disclose secondary usage of data, which is not legal in some countries. On the other hand, firms might obtain the customers' consent for such use, for example, in the form of a complicated data protection declaration, so that the consumer is

Sub-dimension	Description	Measure	Measure levels (ascending commitment)	Related work
Limited/restricted data collection	The collection of (personal) data must be limited, lawful, and fair, usually with the knowledge and/or consent of the user.	Data protection declaration	Detailed; One Pager; Tabular form	[Eu16]; [SMB96]; [Wi21]
Clear purpose of data collection	The purpose of the data collection must be clearly stated at the time of collection.	Communicated purpose of data collection	Contradictory communication; Data protection declaration; At the time of collection	[Di13]; [SMB96]; [Th17]
Restricted data use	The use or disclosure of data must be limited to the agreed purpose(s) or only for closely related purposes.	Secondary usage	Unknown secondary usage; Unintended secondary usage; No secondary usage	[Di13]; [Eu16]; [Wi21]
Openness about data processing practices	Businesses need to be transparent about their data processing practices.	Explanation	Technical/legal explanation; Explanation for layperson; Personalized explanation	[Eu16]; [Wi21]; [TF09]
Secure storage and processing of user data	The storage, processing, and transmission of user data must be subject to appropriate security.	Notification of incidents	On request; Affected users only; Public broadcast	[Eu16]; [Th17]
Data quality	User data collected and stored by companies must be relevant, accurate, and up-to-date.	Connection between data and purpose	No connection; On purpose/data classes; On specific data and purpose	[Ma15]; [Oe13]; [SMB96]
Access and correction	Users must be able to view and correct the user data stored by companies.	Access and correction of personal data	Information; Information and correction; Information, correction, deletion	[Eu16]; [Ma15]; [Th17]

Tab. 2: Overview of privacy and data security sub-dimensions, its exemplary measures, and exemplary related work.

not even aware of his consent and the use of data [Di13], [Wi21]. Accordingly, restricted secondary usage has been exemplarily included in the benchmark corpus

Openness about data processing practices is (partly) covered by the GDPR but also suggested by research to enable consumers to make informed choices and gain some control over their (personal) data [Wi21]. Still, openness can occur in various ways including different levels of explanation which are more or less easy to understand.

The sub-dimension of **secure storage and processing of user data** covers a plethora of possible implementations. Secure storage and processing applies not only to internal (local) utilization but also, for example, to secure data transmission, to the inclusion of other companies in the value creation process. Secure storage and processing goes beyond the mere process in the eyes of the customers. Still, it is mainly perceived in the form of incidents and the related notifications from the consumers' perspective [Th17]. Hence, the notification of incidents concerning stored personal data is included in the benchmark corpus as an example for this sub-dimension.

Data quality can be characterized, amongst other influencing factors, based on the connection between collected data and data collection purpose [Oe13]. This sub-dimension applies to the internal data management processes. Hence, data and initial collection purpose can be stored decoupled from each other, based on formed classes of purposes and data, or for each specific data set with indication of the initial purpose.

The GDPR (partly) covers **access and correction** of personal data. Therefore, this sub-dimension is also captured in the benchmark corpus by its own measure [Ma15], [Th17]. Levels can range from solely information to correction and deletion.

3.2 Evaluating privacy and data security activities within further CDR norms

A more comprehensive approach of privacy and data security exceeds mere activities on the system-level (covered by CDR norm VI "privacy and data security") and rather also impacts other dimensions of CDR. Hence, privacy and data security activities on company-level can also comprise activities rooted in other CDR dimensions (see Table 1 for an overview of the CDR norms). One subordinate possible measure per dimension was developed based on previous research to exemplarily discuss the evaluation of privacy and data security activities on company-level in the context of further CDR norms. Each measure features three different levels to continue the ample-based approach to evaluate CDR activities of companies (see Table 3).

In the context of CDR, the dimension **access** covers the possibility to get in contact with basic digital products and services [HRK08], [LMH17]. Access to everyone is not just strengthening social groups that did not have access until now but also the user experience of all consumers [Ne06]. In this vein, it might be favorable for consumers to be able to access basic services (i.e., advisory services, or (insurance) premium calculators) without providing any personal data. Consumers usually want to protect their personal data and reduce risks from providing such, but often have to weigh this risk against the lack of functionality, known in research as the privacy calculus [AK06], [Ha02], [Su13].

Hence, access related to privacy and data security can be exemplarily included in the benchmark corpus.

Additionally, **education and awareness** should comprise consumers' awareness for ecological, social, and societal aspects as well as the economic impacts of their consumption decisions. This dimension covers a wide spectrum of education fields. Examples are seeking information and advice, or coping with problems [Th17], [Un19]. This demand can even be reinforced through the ongoing digitization and the development of new digital security and privacy technologies. In order to offer secure and privacy-preserving products and services, new technology applications such as blockchain technology are increasingly being used to protect privacy and data security [Ay18], [Wa21]. Thus, associated new concerns arise, for example, regarding energy consumption or sustainability [Tr18], [Wa21]. Furthermore, many consumers are still often unaware of digital products or services intruding upon their privacy, their rights regarding data security and privacy, and how they can make use of them [Lo17], [MDK18]. Thus, education on consumer rights regarding privacy and data security should be offered and is consequently, as an exemplary instance of this dimension, part of the benchmark corpus.

Information and transparency is a broad application field of CDR also covering measures that refer to privacy and data security. For instance, companies can pursue more transparency by adequately informing (potential) customers about the collection, storage, or handling of personal data [Eu16], [TF09] also using certifications [CM20]. As privacy can be regarded as the individual's right, inter alia, to determine whom to disclose personal information [We67], users should be informed about all data processing companies involved in the purchase transaction including process steps such as distribution, packaging, or shipping. Hence, the information on involved companies has been exemplarily incorporated in the benchmark corpus.

Information privacy exceeds the consumers' capability to control their own information stored and the handling of their data especially concerning the monetization of provided data [BC11], [Go91], thus affecting consumers' **economic interests**. In these times, many business models (i.e., freemium, or free distribution through personal data intelligence) rely on analyzing supplied consumer data for own purposes, providing free products and services for the consumer [Lo17]. Hence, consumer data are called the "new currency on the Internet" [Ca12, p. 3834], although consumers might want to protect these sensitive data. Accordingly, the business model used can be decisive for a consumer decision, so consumers should be informed about this. In line with this, this aspect was included as an example for consumers' economic interests in the benchmark corpus.

Motivated by the complications arising from digital products and services, **dispute resolution and awareness** also covers disagreements originating in privacy and data security incidents. In general, dispute resolution refers to the mechanisms aiming to provide consumers who have suffered (economic) harm from transactions, to solve their complaints

CDR norm	Measure	Description	Measure levels (ascending commitment)	Related work
Access	Access without data input	Access, for example, to advisory services, or premium calculators can be open without entering personal data and thus with reduced privacy concerns.	Read only web page content; Limited service without data; Services without data	[AK06]; [LMH17]; [Ne06]; [Su13]
Education and awareness	Consumer rights education	Consumer education regarding their rights related to privacy and data security and how to make use of them.	Not provided; Passive offer; Actively focused	[Lo17]; [MDK18]; [Un19]
Information and transparency	Transparency about business partners	Users should be informed about all data processing companies involved in the purchase transaction.	No information; Hidden information; Proactive information	[Eu16]; [TF09]; [We67]
Economic interests	Deployed business model	Users should know how the company generates revenue with a (free) product or service (e.g., by the usage of collected data).	No information; Hidden information; Proactive information	[BC11]; [Go91]; [MZH19]; [SSL16]
Dispute resolution and awareness	Point of contact	In the event of disagreements originating in privacy and data security, dispute resolution can be secured differently.	Manufacturer specific; Manufacturer network; Independent agency	[Eu16]; [Oe07]; [Th17]

Tab. 3: Overview of further touched CDR norms, its exemplary measures, and exemplary related work.

and receive redress [Oe07]. As digitalization enables companies to operate across borders, the CDR concept envisions an uncomplicated, unified, and efficient dispute resolution and redress mechanism for all consumers. More specifically, CDR suggests that consumers should have the option to place complaints easily and free of charge, while the processing of the complaints should be fast, fair, and transparent [Eu16], [Th17]. The point of contact can have a strong influence on dispute resolution and redress depending on its independence of interests, therefore exemplarily included in the benchmark corpus.

Due to the complex, highly dynamic, and nationally fragmented legal debate on **product safety and liability** of digital products and services [De14], [HTW17] stable safety and liability measures could not be identified yet that would form a solid basis for the evaluation of CDR activities. Nevertheless, future advancements of the benchmark corpus should incorporate this CDR dimension in their considerations.

Because our work focuses on companies and how CDR activities can be evaluated on company-level, the dimension **governance and participation** has been excluded as it lies predominantly in the hands of policymakers and other non-governmental regulatory organizations [Th17]. Since this dimension is out of the direct reach of companies it can be considered to be an exogenous force within a CDR framework and is therefore not part of a benchmark corpus on company-level.

4 Conclusion

The goal of this work-in-progress paper is to start a discussion on how to measure CDR activities on company-level. Especially for companies operating with digital products and services, the understanding of responsibility has changed. The provided benchmark corpus above (see Table 2 and 3) should serve as a starting point for further research, providing exemplary measures to evaluate CDR activities in general and activities related to privacy and data security in particular. Future research should complement, valuate, and validate this part of the benchmark corpus in order to develop a comprehensive evaluation system to assess CDR activities on company-level. In addition, the benchmark corpus covering all dimensions of CDR equally needs to be expanded analogically.

In practice, the provided benchmark corpus should serve as an orientation for firms on how to evaluate privacy and data security activities on company-level. In order to adapt this benchmark corpus to the specific company's environment the applicability of individual measures must be assessed and supplemented with own criteria if needed. Besides, weighting can be used to adapt the benchmark corpus to specific circumstances within the company similar to a utility analysis. In practice, it might be worth considering to align

the status-quo evaluation with internal visions and missions and to create an action plan for the further development based on this benchmark corpus.

A significant limitation is that an all-encompassing benchmark corpus is not feasible even after further developments. Rather, the goal is to find a common, expanded consensus of the most relevant measures through discussion so that a comprehensive application to a wide variety of industries, products, and services is possible. A further development of the benchmark corpus can reduce but not remove this limitation.

5 Acknowledgement

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

6 References

[AK06] Awad, N. F.; Krishnan, M. S.: The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to be Profiled Online for Personalization. MIS Quarterly 30/1, pp. 13-28, 2006.

[Ay18] Ayoade, G. et al.: Decentralized IoT Data Management Using BlockChain and Trusted Execution Environment. In: 2018 IEEE International Conference on Information Reuse and Integration (IRI). Salt Lake City, Utah, USA, pp. 15-22, 2018.

[Ba19] Baumann, A. et al.: The Price of Privacy: An Evaluation of the Economic Value of Collecting Clickstream Data. Business & Information Systems Engineering 61/4, pp. 413-431, 2019.

[BC11] Bélanger, F.; Crossler, R. E.: Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. MIS Quarterly 35/4, pp. 1017-1041, 2011.

[BKV15] Bourreau, M.; Kourandi, F.; Valletti, T.: Net Neutrality with Competing Internet Platforms. Journal of Industrial Economics 63/1, pp. 30-73, 2015.

[Ca12] Camenisch, J.: Information Privacy?!. Computer Networks 56/18, pp. 3834-3848, 2012.

[CM20] Carl, K. V.; Mihale-Wilson, C.: Consumer Privacy Concerns and Preferences for Certification and Accreditation of Intelligent Assistants in the Internet of Things. In (Roßnagel, H.; Schunck, C. H.; Mödersheim, S.; Hühnlein, D. eds.): Open Identity Summit 2020. Gesellschaft für Informatik e.V., Copenhagen, Denmark, pp. 157-162, 2020.

[De14] Desai, D. R.: The New Steam: On Digitization, Decentralization, and Disruption. Hastings Law Journal 65/6, pp. 1469-1482, 2014.

[Di13] Dinev, T. et al.: Information Privacy and Correlates: An Empirical Attempt to Bridge and Distinguish Privacy-Related Concepts. European Journal of Information Systems 22/3, pp. 295-316, 2013.

[DR95] Daughety, A. F.; Reinganum, J. F.: Product Safety: Liability, R&D, and Signaling. American Economic Review 85/5, pp. 1187-1206, 1995.

[Eu16] European Parliament: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance), https://eur-lex.europa.eu/eli/reg/2016/679/oj, access 9 July 2019, 2016.

[Fe19] Felzmann, H. et al.: Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns. Big Data & Society 6/1, p. 2053951719860542, 2019.

[GGK10] Granados, N.; Gupta, A.; Kauffman, R. J.: Research Commentary – Information Transparency in Business-to-Consumer Markets: Concepts, Framework, and Research Agenda. Information Systems Research 21/2, pp. 207-226, 2010.

[Gi18] Gimpel, H. et al.: The Upside of Data Privacy – Delighting Customers by Implementing Data Privacy Measures. Electronic Markets 28/4, pp. 437-452, 2018.

[Go91] Goodwin, C.: Privacy: Recognition of a Consumer Right. Journal of Public Policy and Marketing 10/1, pp. 149-166, 1991.

[GS09] Goel, S.; Shawky, H. A.: Estimating the Market Impact of Security Breach Announcements on Firm Values. Information & Management 46/7, pp. 404-410, 2009.

[Ha02] Hann, I.-H. et al.: Online Information Privacy: Measuring the Cost-Benefit Tradeoff. In (Miralles, F.; Valor, J. eds.): Proceedings of the International Conference on Information Systems 2002, Barcelona, Spain. 2002.

[Ha07] Hann, I.-H. et al.: Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach. Journal of Management Information Systems 24/2, pp. 13-42, 2007.

[He16] Hess, T. et al.: Options for Formulating a Digital Transformation Strategy. MIS Quarterly Executive 15/2, pp. 123-139, 2016.

[HH18] Heimbach, I.; Hinz, O.: The Impact of Sharing Mechanism Design on Content Sharing in Online Social Networks. Information Systems Research 29/3, pp. 592-611, 2018.

[HHS11] Hinz, O.; Hann, I.-H.; Spann, M.: Price Discrimination in E-Commerce? An Examination of Dynamic Pricing in Name-Your-Own Price Markets. MIS Quarterly 35/1, pp. 81-98, 2011.

[HRK08] Hsieh, J. J. P.-A.; Rai, A.; Keil, M.: Understanding Digital Inequality: Comparing Continued Use Behavioral Models of the Socio-Economically Advantaged and Disadvantaged. MIS Quarterly 32/1, pp. 97-126, 2008.

[HTW17] Howells, G.; Twigg-Flesner, C.; Willett, C.: Product Liability and Digital Products. In (Synodinou, T.-E.; Jougleux, P.; Markou, C.; Prastitou, T. eds.): EU Internet Law: Regulation and Enforcement. Springer International Publishing, Cham, pp. 183-195, 2017.

[KBM13] Kesavan, R.; Bernacchi, M. D.; Mascarenhas, O. A.: Word of Mouse: CSR Communication and the Social Media. International Management Review 9/1, pp. 58-66, 2013.

[LMH17] Lameijer, C. S.; Mueller, B.; Hage, E.: Towards Rethinking the Digital Divide: Recognizing Shades of Grey in Older Adults' Digital Inclusion. In (Kim, Y. J.; Agarwal, R.; Lee, J. K. eds.): Proceedings of the International Conference on Information Systems 2017, Seoul, South Korea, 2017.

[Lo17] Lopez, J. et al.: Evolving Privacy: From Sensors to the Internet of Things. Future Generation Computer Systems 75, pp. 46-57, 2017.

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

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

[Ma15] Martin, K. E.: Ethical Issues in the Big Data Industry. MIS Quarterly Executive 14/2, pp. 67-85, 2015.

[MDK18] Manikonda, L.; Deotale, A.; Kambhampati, S.: What's up with Privacy? User Preferences and Privacy Concerns in Intelligent Personal Assistants. In (Furman, J.; Marchant, G.; Price, H.; Rossi, F. eds.): Proceedings of the 2018 AAAI/ACM Conference on AI, Ethics, and Society, New Orleans, LA, USA, ACM, pp. 229-235, 2018.

[Mi21] Mihale-Wilson, C. et al.: Corporate Digital Responsibility – Extended Conceptualization and a Guide to Implementation. In: Proceedings of the 25th European Conference on Information Systems, Marrakech, Morocco, 2021.

[MM08] Matten, D.; Moon, J.: "Implicit" and "Explicit" CSR: A Conceptual Framework for a Comparative Understanding of Corporate Social Responsibility. Academy of Management Review 33/2, pp. 404-424, 2008.

[MR02] Maignan, I.; Ralston, D. A.: Corporate Social Responsibility in Europe and the U.S.: Insights from Businesses' Self-Presentations. Journal of International Business Studies 33/3, pp. 497-514, 2002.

[MZH17] Mihale-Wilson, C.; Zibuschka, J.; Hinz, O.: About User Preferences and Willingness to Pay for a Secure and Privacy Protective Ubiquitous Personal Assistant. In: Proceedings of the 25th European Conference on Information Systems, Guimarães, Portugal, pp. 32-47, 2017.

[MZH19] Mihale-Wilson, C.; Zibuschka, J.; Hinz, O.: User Preferences and Willingness to Pay for In-Vehicle Assistance. Electronic Markets 29/1, pp. 37-53, 2019.

[Na17] Nambisan, S. et al.: Digital Innovation Management: Reinventing Innovation Management Research in a Digital World. MIS Quarterly 41/1, pp. 223-238, 2017.

[Ne06] Newell, A. F. et al.: Designing a Portal for Older Users: A Case Study of an Industrial/Academic Collaboration. ACM Transactions on Computer-Human Interaction 13/3, pp. 347-375, 2006.

[Oe07] OECD: Recommendation on Consumer Dispute Resolution and Redress, http://www.oecd.org/internet/consumer/38960101.pdf, access 9 July 2019, 2007.

[Oe13] OECD: The OECD Privacy Framework, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf, access 9 July 2019, 2013.

[Oe17] OECD: Key Issues for Digital Transformation in the G20. Report Prepared for a Joint G20 German Presidency/OECD Conference, https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf, access 9 July 2019, 2017.

[Sm17] Smith, B. W.: Automated Driving and Product Liability. Michigan State Law Review 2017/1, pp. 1-74, 2017.

[SMB96] Smith, H. J.; Milberg, S. J.; Burke, S. J.: Information Privacy: Measuring Individuals' Concerns About Organizational Practices. MIS Quarterly 20/2, pp. 167-196, 1996.

[SSL16] Stohl, C.; Stohl, M.; Leonardi, P. M.: Managing Opacity: Information Visibility and the Paradox of Transparency in the Digital Age. International Journal of Communication 10, pp. 123-137, 2016.

[Su13] Sutanto, J. et al.: Addressing the Personalization-Privacy Paradox: An Empirical Assessment from a Field Experiment on Smartphone Users. MIS Quarterly 37/4, pp. 1141-1164, 2013.

[Te18] Tesfay, W. B. et al.: PrivacyGuide: Towards an Implementation of the EU GDPR on Internet Privacy Policy Evaluation. In (Verma, R. M.; Kantarcioglu, M. eds.): Proceedings of the Fourth ACM International Workshop on Security and Privacy Analytics, New York, USA, pp. 15-21, 2018.

[TF09] Turilli, M.; Floridi, L.: The Ethics of Information Transparency. Ethics and Information Technology 11/2, pp. 105-112, 2009.

[Th17] Thorun, C. et al.: Indicators of Consumer Protection and Empowerment in the Digital World. Results and Recommendations of a Feasibility Study, https://www.bmjv.de/G20/DE/ConsumerSummit/_documents/Downloads/Studie.pdf?__blob=publicationFile&v=1/, access 9 July 2019, 2017.

[Tr18] Truby, J.: Decarbonizing Bitcoin: Law and Policy Choices for Reducing the Energy Consumption of Blockchain Technologies and Digital Currencies. Energy Research & Social Science 44, pp. 399-410, 2018.

[Un19] United Nations: Manual on Consumer Protection, https://unctad.org/en/PublicationsLibrary/ditccplp2017d1_en.pdf, access 12 November 2020, 2019.

[VS13] Venkatesh, V.; Sykes, T. A.: Digital Divide Initiative Success in Developing Countries: A Longitudinal Field Study in a Village in India. Information Systems Research 24/2, pp. 239-260, 2013.

[Wa21] Waheed, N. et al.: Security and Privacy in IoT Using Machine Learning and Blockchain: Threats and Countermeasures. ACM Computing Surveys 53/6, pp. 1-37, 2021.

[We67] Westin, A. F.: Privacy and Freedom. 1st ed., Athenum, New York, 1967.

[Wi21] Wieringa, J. et al.: Data Analytics in a Privacy-Concerned World. Journal of Business Research 122, pp. 915-925, 2021.