RESEARCH IN PROGRESS

CONCEPTUALIZING THE IMPACT OF DIGITAL BUSINESS MODELS ON PRIVACY CONCERNS

MIRANDA KAJTAZI,[1] ERDELINA KURTI[2, 3]

[1] Lund University, School of Economics and Management, Department of Informatics, Lund, Sweden
miranda.kajtazi @ics.lu.se
[2] Malmö University, Faculty of Technology and Society, Department of Computer Science and Media Technology, Malmö, Sweden
erdelina.kurti@mau.se
[3] Linnaeus University, Faculty of Technology, Department of Informatics, Växjö, Sweden
erdelina.kurti@lnu.se

Digital technologies have enabled novel forms and reconfigurations of value creation, delivery, and capture. These new reconfigurations challenge the conventional notion of value creation with digital business models. On that premise, the widening of privacy concerns, alert us that organizations of the elite digital, like Netflix, Amazon, and Spotify, design technology to feed on personal data, based on algorithmic profiling capabilities. Then, privacy itself becomes their digital business model. In this paper we conceptualize the impact of digital business models on privacy concerns, by presenting a focused literature review that presents 4 waves of research on understanding privacy from the context of digital business models. With our initial findings, we recommend that future technological development should pay central attention to privacy-preserving digital business models, by making it possible that data privacy is envisioned with the right safeguards, targeting 'invisibility' of the user.

Keywords:
digital business models, privacy concerns, value creation, invisibility, right safeguards

University of Maribor Press

DOI https://doi.org/10.18690/um.fov.6.2023.43
ISBN 978-961-286-804-8

1 Introduction

The exponential advancement and widespread utilization of digital technologies has spawned profound innovations, which have disrupted traditional businesses and reconfigured a number of industries (Nambisan et al., 2020). Digitization, which is defined as the conversion of analog data to digital (Yoo et al., 2010), of products and services, is the cornerstone of innovations, which transcend geographical and industrial boundaries enabling novel business models (Constantinides et al. 2018; Nambisan et al., 2020). A business model represents a key source of performance and competitive advantage of organizations (Teece, 2010), hence becoming an imperative for digital transformation. It refers to the "architecture of value creation, delivery and capture mechanism" (Teece, 2010, p.172), in a multi-actor network. The core of business models is on value creation and capture, not only for the organization itself, but also for other actors in the ecosystem (Amit and Zott, 2020).

For organizations, the advent of information technology (IT) in the 1990s became a ground to breed a new generation of entrepreneurs that redefined the rules of doing business, primarily on the basis of competition, facilitated by IT (Gordon, 2000). On that end, the dot com bust in the 2000s, mandated a few entrepreneurs to reinvent the use of IT by crafting a new economic order (Zuboff, 2015). Pioneers like Netflix, Amazon, and Spotify, started to become the best attendants of feeding on personal data (Loebbecke and Picot, 2015), with a constant online surveillance, often without the knowledge of a person (Zuboff, 2019). The legal enforcement, however, with the ratification of the General Data Protection Regulation (GDPR) as the most powerful regulation ever created, presented a shift in the mind-set of how data protection is handled by such organizations. In this paper, we look at digital business models vis-á-vis privacy concerns, with the aim to provide an initial conceptual model on the interplay of digital business models and privacy concerns, over time.

The rest of the paper is organized as follows. We first present our conceptualizations on digital business models and privacy. We then present a focused literature review followed by an initial conceptualization to view privacy as a direct consequence of reconfigurations of business and the growth of digital business models. We then highlight potential contributions of our initial conceptualization, followed by future work.

2 Digital Business Models and Privacy Concerns

Digital technologies have enabled novel forms and reconfigurations of value creation, delivery, and capture. These new reconfigurations challenge the conventional notion of value creation, postulating that value is co-created by "aggregating recombinant technology components by interacting with diverse resources and often across firm boundaries" (Hukal and Henfridsson, 2017 p. 488). As a result, the notion of digital business model has gained widespread popularity both in scholarly work, but also in practice. Digital business models refer to business models enabled by the utilization of digital technologies (Amit and Zott, 2020). Bärenfänger and Otto (2015, p. 18) define digital business models "as a business model whose underlying business logic deliberately acknowledges the characteristics of digitization and takes advantage of them; both in interaction with customers and business partners, and in its internal operations".

In consideration of the foregoing, it is no surprise that we have now reached a point when digital business models have influenced the generation of an organizational mind-set that even knows our deepest secrets (Acquisti et al., 2022; Zuboff, 2019). The value of personal information has made it possible for goods to increase prices tenfold on personalized services. Even the simplest case of M&M's legendary milk chocolate candy pack is no stranger to that. M&M owns a platform that allows you to personalize a chocolate pack, where you share personal information, e.g. dates and photographs, taking the opportunity of such data to turn it into a commodity (Crain, 2016). That also allows such platforms not only to influence our future consumer behavior, it also allows for an astronomical price tag, all made possible by the new wave of digital business models configured for personalization.

Then, it is not new to us that IT has become a constant in reconfiguring traditional roles of people in the digital realm, including their traditional view on privacy concerns (Zhang et al., 2022). Organizations driven by information capitalism (Zuboff, 2019), especially the elite digital, show an unstoppable appetite for data that forms 95% of the global economy (Srnicek, 2017). From a macro perspective, the digitization of an organization presented an opportunistic reality (Thrift, 2011) where concepts like "everyware" (Greenfield, 2006) came to life. From a micro perspective, however, secrecy in such organizations came at the expense of privacy (Solove, 2011). Zubbof's "big other" became a precondition to argue that we are in the hands of a new form of capitalism that she termed surveillance capitalism (Zuboff, 2015), where personal boundaries on our own privacy are put to test (Zhang et al., 2022).

Contrary to this view, we know that digitization is key to produce a number of digital business models that deserted the spatial and temporal limits, often empowering people. Just to name a few, from the speed of information, to the significance of online payments for simple transactions, technological capabilities can steer progress in the right direction. However, the digital era is a new reality for people that has brought us more tension than consensus, putting people's own privacy-protective behaviors to test (Quach et al., 2022; Zhang et al., 2022). We live with pressure trying to balance our and others' physical presence with the digital presence (Acquisti et al., 2022). Alongside the backdrop of this pressure, digital business models are leading us to conceptualize our personal digital self as a type of self that transcends the borders and acknowledges our physical self, often recognizing privacy as a loss in that transcension (Zuboff, 2019).

2.1 Focused Literature Review: Digital Business Models and Personal Boundaries on Privacy

In a focused literature review, we identify 22 research articles (listed in Appendix) published at the European Journal of Information Systems (EJIS) in the course of 3 decades. The focus on EJIS stems from their distinctive European perspective on theory and practice for a global audience. Coupled with European Union laws and regulations on data privacy, such as GDPR, it makes for a unique candidate to study the conceptualization of digital business models vis-á-vis privacy concerns, over time. The article analyses yielded 4 waves of research on understanding privacy from the context of digital business models. Important to highlight, is the fact that all articles recognize that privacy is a human right, but the difference across the waves is noticed on the fact that early studies have the tendency to conceptualize on privacy concerns from the user perspective, compared to current studies that place a lot of responsibility on the design of IT itself. Wave 1, presented the early take on the use of digital business models, such as in the form of e-commerce and social media from a network perspective, where privacy conceptions were formed around the "*user privacy concern*" (e.g. Junglas et al., 2008), where personal privacy and the identifiable person were key, along with the data rights, but centered on the actual "user x".

Wave 2 presented the wake of new digital business models that further fueled the presence and use of e-commerce and social media for more personalized services, including services for personal digital healthcare, which influenced a complex analysis on privacy as e.g. a right and commodity (Smith et al., 2011). This made it critical to view "*user disclosure and personalization*" as a real physical person and that data and information disclosure became pivotal to our understanding of privacy concerns (Posey et al., 2010; Warkentin et al., 2011). Wave 3, showed that new techniques on big data analyses with machine learning algorithms, made it more concerning that "*personal data and privacy loss*" is a real threat (Parks et al., 2017). Then, wave 4 and the current wave, focuses on important aspects, such as traceability and integrity (Raddatz et al., 2021; Parks et al., 2022), where a clear motivator for such studies depends on the movements of human rights perspective, where "*personal privacy rights*" are linked back to laws and regulations. In fact, the focus on privacy as a fundamental human right (UN Declaration of Human Rights, Article 12), is key to guide recent studies on design of technology for privacy protection and privacy-preservation mechanisms. Figure 1 illustrates these waves with an example where user x is identified as Sarah Smith, which leads to show how the other waves address privacy concerns, over time.

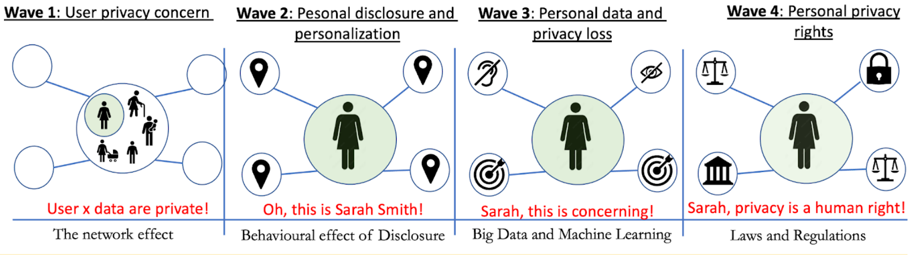
Wave 1: User privacy concern
Wave 2: Pesonal disclosure and personalization
Wave 3: Personal data and privacy loss
Wave 4: Personal privacy rights
User x data are private!
Oh, this is Sarah Smith!
Sarah, this is concerning!
Sarah, privacy is a human right!
The network effect
Behavioural effect of Disclosure
Big Data and Machine Learning
Laws and Regulations

Figure 1: From User Privacy to Privacy as a Right

In reference to these waves, our analysis identified several types of digital business models studied in these waves, e.g. platform business models of e-commerce or data-driven business models; etc. In describing Figure 1, we conceptualize them as digital business models. Such digital business models rely on digital technologies, which contribute to the generation and proliferation of data, which has recently exceeded in growth and profit (Wiener et al., 2020).

As such, digital business model- dependent organizations have harnessed the potential of digital technologies to create novel reconfigurations of value creation and capture, either through novel offerings, reconfiguration of activities, transactions, structure and/or governance mechanisms (Amit and Zott, 2020), all dependent on personal data feeding. To that end, successful organizations as Netflix, Amazon, and Spotify, have configured their business models and innovations around data. Netflix for example, has shifted its focus from a retailer of DVDs mail delivery to innovating its business model around data to improve customer experience through personalization and customization (Mier and Kohli, 2021). The common link across these organizations is that their business models are configured and innovated as data dependent digital platforms. The latter leads us to reflect back on how privacy concerns have shifted from conceptualizing about the unknown "user x" to the actual "physical person".

3 Initial Findings and Future Research Direction

Despite the fact that we have ample opportunities with the introduction and exponential growth of digital business models, and that new IT developments present ideas, tools, and models with privacy-preserving mechanisms, we identify that challenges with data privacy still remain detrimental. Novel configurations of digital business models where privacy becomes the core value creation mechanism, leads us to term them as privacy-based business models. In this relationship, privacy itself becomes the business model. We recommend future technological design to focus on privacy-preserving digital business models, which should make it possible that data privacy is envisioned with the right safeguards, targeting 'invisibility'. Otherwise, Mann's and Matzner's (2019) call that we risk producing technology that does not account for privacy and data protection rights, goes against GDPR's call on the 'right' not to be ruled by automated decisions. Our future work depends on bringing the question of ethics into view, on how technology is shaped to feed on personal data, where user awareness and digital literacy remain challenging. The vast majority of today's digital users have limited awareness about algorithmic profiling capabilities and how detrimental its effects are on their privacy. At the same time, these users have become pivotal in supporting data-driven business models to thrive, letting such models to feed on their valuable personal data.

Acknowledgements

This paper is partially funded by the Crafoord Foundation with project number 20200668.

References

Acquisti, A., Brandimarte, L., Hancock, J. (2022). How privacy's past may shape its future. Science, 375(6578), 270-272.

Amit, R., Zott, C. (2020). Business Model Innovation strategy: Transformational Concepts and Tools for Entrepreneurial Leaders. John Wiley & Sons: Hoboken, NJ, USA.

Bärenfänger, R., Otto, B. (2015). Proposing a capability perspective on digital business models. In 2015 IEEE 17th Conference on Business Informatics, 1, 17-25.

Crain, M. (2016). The limits of transparency: Data brokers and commodification, New Media and Society, 20(1), 88-104.

Gordon, R. J. (2000). "Does the "New Economy" Measure Up to the Great Inventions of the Past?" Journal of Economic Perspectives, 14(4), 49-74.

Greenfield, A. (2006) Everyware: The Dawning Age of Ubiquitous Computing, New Riders, Boston, USA.

Hukal, P., Henfridsson, O. (2017). Digital Innovation—A definition and integrated perspective. In The Routledge Companion to Management Information Systems, 1st ed.; Routledge: London, UK, 2017; pp. 360–369.

Junglas, I.A., Johnson, N.A., Spitzmüller, Ch. (2008). Personality traits and concern for privacy: an empirical study in the context of location-based services. European Journal of Information Systems, 17, 387-402.

Loebbecke, C., Picot, A. (2015). Reflections on societal and business model transformation arising from digitization and big data analytics: A research agenda. The Journal of Strategic Information Systems, 24(3), 149-157.

Mann, M., Matzner, T. (2019). Challenging algorithmic profiling: The limits of data protection and anti-discrimination in responding to emergent discrimination. Big Data & Society, 1-11.

Mier, J. & Kohli, A.K. (2021). Netflix: reinvention across multiple time periods, reflections and directions for future research. AMS Review, 11, pp.1-12.

Parks, R., Xu, H., Chu, Ch-H., Lowry, P.B. (2017). Examining the intended and unintended consequences of organisational privacy safeguards. European Journal of Information Systems, 26, 37-65.

Parks, R. F., Wigard, R. T., Lowry, P.B. (2022). Balancing information privacy and operational utility in healthcare: proposing a privacy impact assessment (PIA) framework. European Journal of Information Systems, 1-18.

Posey, C., Lowry, P.B., Roberts, T.L., Selwyn Ellis, T. (2010). Proposing the online community self-disclosure model: the case of working professionals in France and the U.K. who use online communities. European Journal of Information Systems, 19, 181-195.

Quach, S., Thaichon, P., Martin, K.D., Weaven, S., Palmatier, R.W. (2022). Digital technologies: tensions in privacy and data. Journal of the Academy of the Marketing Sciences, 50, 1299-1323.

Raddatz, N., Coyne, J., Menard, Ph., Crossler, R.E. (2021). Becoming a blockchain user: understanding consumers' benefits realization to use blockchain based- applications. European Journal of Information Systems, 1-28.

Smith, J.H., Dinev, T., Xu,H. (2011). Information Privacy Research: An Interdisciplinary Review. MIS Quarterly, 35(4), 989-1015.

Srnicek, N. (2017). The challenges of platform capitalism: Understanding the logic of a new business model, Juncture, 23(4), 254-257.

Teece, D.J. (2010). Business models, business strategy and innovation. Long Range Planning, 43, 172–194.

Wiener, M., Saunders, C., Marabelli, M. (2020). Big-data business models: A critical literature review and multiperspective research framework. Journal of Information Technology, 35(1), 66-91.

Zhang, N., Wang, Ch., Karahanna, E., Xu, Y. (2022). Peer Privacy Concerns: Conceptualization and Measurement. MIS Quarterly, 46(1), 491-530.

Zuboff, Sh. (2015). Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30, 75-89.

Zuboff, Sh. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power, Profile Books, UK.

Appendix

No	Citation	Key Focus of the Study	Context of Information Systems	Context of Data/Information	Theoretical Foundation
1	Parks et al. (2022)	Information privacy threats and maintaining utility in a healthcare privacy compliance context with value-focused thinking (VFT) approach.	eHealth	Patient Information	Means-end chain theory Value-Focused thinking approach
2	Raddatz et al. (2021)	Blockchain as data store to promote data privacy, transaction integrity. Factors that influence consumers' perceptions of blockchain-based databases' benefits	Blockchain databases	Transactional data, personal data	Blockchain research Health belief model Perceived benefits of blockchain-based databases
3	Lin, Carter & Liu (2021)	Contact tracing technology, citizen information privacy concerns.	Smartphones, contact tracing-apps	Information privacy ("the ability of individuals to control the terms under which their personal information is acquired and used" p.389)	Information Privacy Technology Adoption
4	Dincelli & Chengalur-Smith	Gamified SETA artefact using the formats of text and visual to identify security threats.	Social networking sites (SNS) Social engineering Gamification	Data privacy	Online self-disclosure (OSD) Attitudes and intentions towards OSD behavior

No	Citation	Key Focus of the Study	Context of Information Systems	Context of Data/Information	Theoretical Foundation
		Provides an understanding of the linkage between technology artefacts and human experiences.	SETA		SETA and gamification
5	Trang et al. (2020)	Contact-tracing apps during the pandemic. Mass acceptance.	Contact-tracing apps Mobile technology	Contact data	Benefits of tracing apps Appeals for prosocial behavior Constant usage and usability requirements Sensitive data and privacy concerns App acceptance, user-centered design
6	Rowe, Nqwenyama & Richet (2020)	The failure in the design and adoption of Stop-COVID app in France. Conditions of such failure.	Tracing, smartphone app	Collection of data	E-GOV Apps for crisis management Alienation in critical theory
7	Ozdemir, Smith & Benamati (2017)	Information privacy in the context of peer relationships on commercial social media sites. A model that considers relationships between the constructs of privacy experiences.	Social media	Personal information	Privacy research Privacy-related constructs Information disclosure
8	Lowry, Dinev &	Important concerns in the	IS Research	Big data	IT artefacts to IS artefacts

No	Citation	Key Focus of the Study	Context of Information Systems	Context of Data/Information	Theoretical Foundation
	Willison (2017)	hope of improving the effectiveness of security and privacy research. Outlines three promising opportunities for IS research that is compelling to security and privacy researchers.			Security and privacy research Opportunities – online platforms, IoT, big data
9	Parks et al. (2017)	Investigate the consequences of privacy safeguard enactment in medical practices, including whether it influences their ability to meet privacy requirements and whether workflows are impeded	Health informatics	Information privacy	Health informatics Privacy safeguards in healthcare The intended versus unintended consequences of enacting privacy safeguards in organizations.
10	Foth (2016)	Analyzed the influences of the attitudes, subjective norms and perceived behavioral control on employees' intentions to comply with data protection regulations.	Health care systems	Data protection	Information security
11	Bansal, Zahedi & Gefen (2015)	Important website features: privacy policy statements + privacy	Internet, websites	Collection of data	Privacy Concern, Trust, and Privacy Assurance

No	Citation	Key Focus of the Study	Context of Information Systems	Context of Data/Infor-mation	Theoretical Foundation
		assurance cues are what online providers use to increase individuals' trust and willingness to disclose private information online. Comprehensive examination of the process by which privacy assurance mechanisms □ influence trust and the moderating role of privacy concern in this process			
12	Chen & Sharma (2015)	Facebook users' learning-based attitude formation and the relationship between member attitude and self-disclosure.	Social media	Data in social network	Self-disclosure Social networking sites Attitude literature
13	Roßnagel et al. (2014)	Determinants for success and failure of identity management systems. Analyze the preferences and willingness to pay of prospective users.	Identity management systems	User data	Success factors of we identity management solutions

No	Citation	Key Focus of the Study	Context of Information Systems	Context of Data/Information	Theoretical Foundation
14	Oetzel & Speikermann (2014)	Methodology that systematically considers privacy issues by using a step-by-step privacy impact assessment.	IT applications	Data protection	Existing privacy compliance procedures and privacy-by-design Risk assessment methodologies that tackle security and privacy issues PIA
15	Miltgen & Peyrat-Guillard (2014)	Examines how European citizens decide to disclose and protect their personal data and thereby reveals cultural and generational divides.	NA.	Information privacy	Information privacy Situationally Antecedents and consequences The importance of trust Privacy-related issues
16	Dinev (2014)	Privacy in the information age, future opportunities for research.	IT, e-commerce, social networks	Personal data	Privacy definition and conceptualization Anthropological and cultural angle of privacy Regulation Privacy and convenience. Privacy paradox
17	Dinev et al. (2013)	Develops and tests a framework of information privacy and its correlates, the latter often being confused with or built into definitions of information privacy per se.	NA.	Information privacy	The concept of privacy – literature review

No	Citation	Key Focus of the Study	Context of Information Systems	Context of Data/Information	Theoretical Foundation
18	Li & Unger (2012)	Perceived personalization quality can outweigh the impact of privacy concerns. Service providers can improve the perceived quality of personalization services being offered in order to offset customer privacy concerns.	Personalization applications	NA.	Personalization Customers' privacy concerns Privacy protection
19	Warkentin, et a.. (2011)	Investigates the antecedents of information privacy policy compliance efficacy □ by individuals.	Healthcare systems?	Personal data, sensitive data?	Social learning theory Compliance
20	Posey et al. (2010)	An online community self-disclosure model, tested in a cross cultural setting using data provided by French and British working professionals	Online communities, social networking	NA.	Social exchange theory Social penetration theory Cross-cultural theory related to individualism-collectivism
21	Junglas et al. (2008)	Fill the gap of "research has shown that the CFP can have a negative influence on the adoption of information technology; but	World wide web	NA.	Concern for privacy (CFP) The co-evolving nature of privacy and technology PMT and threat appraisals Personality traits and threat appraisals

No	Citation	Key Focus of the Study	Context of Informatio n Systems	Context of Data/Infor-mation	Theoretical Foundation
		little is known about factors likely to influence such concern."			
22	Dinev et al. (2006)	Examines cross-cultural differences beliefs related to e-commerce use for Italy and the United States.	NA.	Personal information Information privacy concerns	Internet and e-commerce diffusion in Italy Hofstede's cultural theory Fukuyama's theory of trust and social capital