Journal of Business Models (2022), Vol. 10, No. 2, pp. 31-57

JOURNAL OF BUSINESS MODELS

The Role of Privacy Protection in Business Models for Sustainability: A Conceptual Integration from an Ecosystem Perspective

Fabien Rezac[1]

Abstract

Purpose: The principal purpose of this article is to address a critical issue emerging in the realm of interorganizational dependencies heavily impacted by digitalization, namely developing business models that would protect privacy in a sustainable way. On the one hand, companies have been jointly proposing, creating, delivering, and capturing value through an excessive, unethical exploitation of personal data and information. On the other, restricting and controlling flows of data and information hampers the processes that lead to social well-being. This article reflects on this paradox by building on the theories of business models for sustainability and contextual integrity, while offering a holistic conceptual narrative guiding the sustainable transition towards digital equity and inclusivity.

Design/methodology/approach: This conceptual article can be classified as a theory synthesis paper with the ambition to achieve an outcome that enhances knowledge on concepts and a phenomenon by a conceptual integration across two different, previously unconnected literature streams and theories.

Findings: This article suggests that businesses which play any role in transmission of data and information cannot be sustainable without protecting privacy as a social value. Furthermore, it argues that privacy cannot be protected without addressing the appropriateness of both flow and use of data and information with respect to all involved stakeholders. Ultimately, via linking two distinct yet interrelated and rigorously developed research streams, a heuristic framework for privacy and sustainability in business models is proposed as a system of key considerations for managers to apply in assessing and planning a business practice, so it protects privacy in a sustainable way.

Originality/value: The key theoretical contribution of this article can be considered twofold. Firstly, it unfolds the relevance of privacy protection for the stream of business model research directed toward sustainable development in a way that is theoretically rigorous, complementary with the stakeholder theory, and reflecting the changing interorganizational dependencies affected by digitalization. Secondly, it contributes to the contemporary debate on privacy as a social value through identifying theoretically thorough avenue for adapting the theory of contextual integrity to a social domain where value proposition, creation, delivery, and capture with and for stakeholders involves transmission of data and information.

Keywords: Privacy, privacy protection, contextual integrity, ecosystems, sustainability, social sustainability, business models, business models for sustainability

Please cite this paper as: Rezac, F. (2022), The Role of Privacy Protection in Business Models for Sustainability: A Conceptual Integration from an Ecosystem Perspective, Journal of Business Models, Vol. 10, No. 2, pp. 31-57

1 Aarhus University, Denmark

ISSN: 2246-2465

DOI: https://doi.org/10.54337/jbm.v10i2.6952

Introduction

It is obvious that data-driven technologies have significantly impacted the way how business is conducted (e.g., Johnson, Christensen and Kagermann, 2008; Amit and Zott, 2012; Iansiti and Lakhani, 2014; Porter and Heppelmann, 2015). Literally every aspect of the business landscape has been radically shifting (Westerman and Bonnet, 2015) and with the Fourth Industrial Revolution underway, the biological, physical, and digital worlds have been gradually fusing. People have never been so close to technology before (Schwab, 2016; Rigby, 2014) and, in fact, each of us can now be considered a "walking data generator" (McAfee and Brynjolfsson, 2012, p. 63). Just to illustrate, it is estimated that by 2023, there will be 29.3 billion networked devices, which is approximately 10 billion more than 5 years earlier (Cisco, 2020). With the contribution of the COVID-19 pandemic causing a sudden increase in online presence, more than 59 zettabytes of data were predicted to be created, captured, copied, and consumed solely in 2020 (IDC, 2020). This amount of data is expected to grow with a five-year compound annual growth rate of 26 percent through 2024, and despite the ratio of unique data to replicated data being approximately 1:9, the data created by 2023 will amount for creation of more data than in the past 30 years (IDC, 2020). In the same breath, however, it is necessary to add that technology per se has no single objective value (Chesbrough, 2010) and the same applies to all the data it generates. These barely imaginable volumes mean nothing unless they are processed and used for various purposes – including those of commercial character.

Generally, business environments consist of interdependent bundles of resources, markets and technologies controlled by many (Astley and Fombrun, 1983). Therefore, when proposing, creating, delivering, and capturing value, we can see companies navigating these nowadays highly digitalized spaces jointly, by managing such dependencies with focus on establishing complementarity. On the one hand, they do so by actively engaging in different networks where the interorganizational relationships are governed by an interplay of contractual and relational mechanisms (Aagaard and Rezac, 2022). On the other, we can also see companies becoming embedded in ecosystems – sets of actors with varying degrees of multi-lateral, non-generic complementarities that are not fully hierarchically controlled and cannot be decomposed into an aggregation of bilateral interactions (Jacobides, 2019; Shipilov and Gawer, 2020; Adner, 2017). Underpinned by modularity, the jointly created value ultimately covers customer needs broader than the needs an individual firm would be ever able to address in isolation. Thus, facing the reality that offering alternative value proposition has little or no effect on building up a competitive advantage, the innately self-interested companies cope with the major paradigm shift by co-specializing and opening up for collaboration even with their competitors (Jacobides, Cennamo and Gawer, 2018; Gnyawali and Charleton, 2018, Jacobides, 2019).

Zooming in on the dynamics of ecosystems in particular, we can see companies co-creating products and services that span the traditionally clearly demarcated organizational as well as industrial boundaries – typically by using digital platforms, Application Programming Interfaces, Internet of Things, and other tools for gathering, sharing and analysing data (Desai, Fountaine and Rowshankish, 2022; Fuller, Jacobides and Reeves, 2019, Porter and Heppelmann, 2014). And while there is no doubt that such a substantial data-driven progress has all the required potential to serve as a major catalyst for socially sustainable development, it simultaneously encompasses a number of critical concerns, with privacy protection being one of the most imperative (e.g., Acquisti, Taylor and Wagman, 2016; World Economic Forum, 2021; Gstrein and Beaulieu, 2022). The endless array of notorious scandals of big-tech behemoths has drawn attention to the colossal imbalance of the value created for companies compared to value created for society. It has become widely recognised that organizations capitalize on customers' personal data and often use it on a massive scale without their permission or awareness (cf. Cochrane, 2018; Burt, 2019). Despite the fierce deployment of various regulatory mechanisms the mitigation by external interventions seems to be ineffective or, in fact, even counterproductive for innovation per se (cf. Bansal, Zahedi and Gefen, 2015; Burt, 2018; Martin, Matt, Niebel and Blind, 2019). While the infamous trade-off between customers' convenience versus their privacy gradually escalates into a crisis of society-wide proportions (e.g., Meyer and Kirby, 2010; Li and Unger, 2012; Wang, 2013; Cloarec, 2020), the business models of many paradigm-setting companies still rely on exploitation of data and information, essentially ignoring their cumulative impact on the social bottom line. Since their products and services embody the very cornerstone of some of the most fundamental daily-life operations, giving up privacy has become seen simply as an inevitable collateral damage of living in this day and age – an ordinary price expected to be paid to be able to fulfil one's basic needs.

The practice of leveraging data for the commercial purpose has become so far-reaching that some researchers even resorted to using terms as expressive as "data capitalism" (West, 2017, p. 20). And although the rise of distributed-ledger created a number of opportunities for levelling out the playing field and establishing digital sovereignty (Montes and Goertzel, 2019), reclaiming the ideals that revolve around the notion of human-centricity requires to stop applying intrusive techniques and find a safer, more inclusive way to develop business (Esteve, 2017; Caputo, Pizzi, Pellegrini and Dabić, 2021). The current status quo residing in pseudo-competition dominated by gatekeeping platforms gradually closing their ecosystems and perpetually reinforcing their walled gardens calls for revisiting privacy protection from a perspective that reflects the current situation underpinned by redefined interorganizational dependencies. On the one hand, it is desirable for customers to share data and information – it makes their life swiftly convenient. On the other, however, one must simultaneously consider the picture in full; when used for generating profit across ecosystems, the data and information must be combined and used only in ways that are sustainable not only for an individual but also for the society at large.

This article attempts to tackle the abovementioned issue by answering the research question "How can companies propose, create, deliver, and capture value while protecting privacy in a sustainable way?" and unfolds followingly. First, due to the generally ambiguous understanding of conceptual articles, the applied process is delineated by presenting the deliberations that constitute the research design. Second, most relevant debates on the topic of concern are introduced and, adopting a perspective that reflects the current multilaterality of interdependencies in the digitalized world, the main limitations stemming from the nexus of the respective concepts are identified. Third, the concepts are integrated and a heuristic framework for sustainable privacy protection through business models is presented. Finally, the article reflects on the presented contribution in terms future research and managerial implications.

Research Design

As Salomone (1993, p. 73) puts it, "a sound conceptual article can be a quantum leap, in terms of value and usefulness, beyond a typical literature review." Overall, as pointed out by Gilson and Goldberg (2015), the difference between a review and a conceptual paper is the question "what's new." Although a conceptual article should include a concise overview of the domain that also describes the state of the affairs in the scientific field in question (i.e., "what do we know, where have we come from, and what are the areas yet to be examined," p. 128), this section should be written in a concise fashion, allowing the author to focus on a specific area that requires attention as well as propose and integrate relationships between constructs that have not been tested before. Although a conceptual article should include a concise overview of the domain that also describes the state of the affairs in the scientific field in question (i.e., "what do we know, where have we come from, and what are the areas yet to be examined," p. 128), this section should be written in a concise fashion, allowing the author to focus on a specific area that requires attention as well as propose and integrate relationships between constructs that have not been tested before. Although the distinction between empirical and conceptual articles is commonly drawn through the assumption that empirical articles have data while conceptual ones do not, not all papers without data are considered to be conceptual (Elder and Paul, 2009; MacInnis, 2004; Cropanzano, 2009).

The understanding of conceptual papers applied throughout this manuscript can be considered in line with a recently published contribution by Jaakkola (2020). This article concurs with her proposition that "a well-designed conceptual paper must explicitly justify and explicate decisions about key elements of the study" (p. 19) and shares her view on the research design elements a conceptual paper should comprise. Firstly, the argumentation in conceptual literature is based "less on data in the traditional sense, but involve the assimilation and combination of evidence that may come from a variety of sources" (Hirschheim, 2008, p. 434); therefore, it is necessary to be explicit about the choice of theories and concepts used to generate novel insights, which could be based on either a focal phenomenon or a focal theory. Furthermore, the authors should clarify their choice of theories and concepts that are being analysed and draw distinction between domain theory (i.e., "particular set of knowledge on a substantive topic area situated in a field or domain") and method theory (i.e., "meta-level conceptual system for studying the substantive issue(s) of the domain theory at hand") (Lukka and Vinnari, 2014). Other elements necessary to consider are the level of perspective, level of analysis, level of aggregation, key concepts used for analysis and explanation, key concepts to be analysed and explained, translating the focal phenomenon in a conceptual language, method of integrating the well-defined concepts, and quality of argumentation (Jaakkola, 2020, p. 20).

As presented further on, the approach towards reviewing literature in writing this article has been predominantly focused on two pertinent research streams, i.e., business models for sustainability and privacy. In both cases, the respective streams have been traced to their very inception and, searching for potential parallels, a theoretical narrative highlighting their emerging complementarity have been developed. Resultingly, adopting an ecosystem angle, this effort allowed for discovering a crucial significance of relating privacy protection to business models that are directed toward sustainable development. This phenomenon focal to the contribution of this article is observable, but not adequately addressed in the extant research (i.e., literature on sustainability in business models and literature exploring with privacy as a social value). The key concepts (i.e., business models for sustainability, contextual integrity) were chosen based on the fit with the phenomenon. Furthermore, due to the complementarity of these concepts, an interdisciplinary synthesis has been found exceptionally promising to address the emerging blind spots in both streams. While empirically interrelated, the research focused on privacy as a social value has foundations in philosophy and does not address business in combination with sustainability, while research on sustainability in business is rooted in management and does not address privacy as a social value in a way that would reflect privacy as a self-contained concept. The selection of papers used for building the argument has, therefore, been based on their relevance to the focal phenomenon and the conducted synthesis. The overview of choices related to this paper are illustrated in Table 1.

Adopting a perspective that takes into account the differences in methodological approach (i.e., how the argument is structured) introduced by Jaakkola (2020), this article can be classified as a synthesis paper, i.e., an article with the ambition to achieve an outcome that enhances knowledge on a concept or a phenomenon by conceptual integration across different, previously unconnected literature streams or theories. To elaborate, adopting the typology of conceptual contributions developed by MacInnis (2011), the general conceptual goal of this article is to relate the concepts of business models for sustainability and contextual integrity by integrating them, i.e., "seeing the simplicity from the complex" (p. 146). The process of integration requires linking the previously unconnected phenomena, seeking a parsimonious and higher-order perspective unfolding the previously unexplored relations. The role of authors is to act as metaphorical "architects" who project an original building from a set of materials through portraying the construction as a whole, while pointing out how the individual elements fit together in an unprecedented way.

Table 1.

Empirical research	Conceptual paper equivalent	Research design elements of this article
Theoretical framing	Choice of theories and concepts used to generate novel insights	Privacy protection in sustainable business models from an ecosystem perspective
Data (source, sample, method of collection)	Choice of theories and concepts analysed	Business models for sustainability, contextual integrity
Unit of analysis	Perspective; level(s) of analysis/ aggregation	Meta-perspective
Variables studied (independent/dependent)	Key concepts to be analysed/explained or used to analyse/explain	Sustainable privacy protection in business models
Operationalization, scales, measures	Translation of target phenomenon in conceptual language; definitions of key concepts	Based on a thorough review of relevant literature
Approach to data analysis	Approach to integrating concepts; quality of argumentation	Figure 1.

Table 1: Decisions about the key elements of this study in accordance with Jaakkola (2020)

Understanding Business Models for Sustainability

Although there seems to be a consensus that the motivation of business model research is to systematically and holistically explain how companies do business (Zott, Amit and Massa, 2011), how it is run, and how it is developed (Spieth, Schneckenberg and Ricart, 2014); it is still apparent that the research area suffers from a significant ambiguity caused by a high number of different conceptualizations as well as taxonomies that systematically classify them. To cite Teece, "there are almost as many definitions of a business model as there are business models" (Teece, 2018, p. 41). Although the concept of business models has evolved extensively over the last two decades, it is still being referred to as an "unclear idea with a cannibalizing tendency towards other management terms" (DaSilva and Trkman, 2014, s. 379). On the other hand, explaining its importance for the field of business and management, Massa, Tucci and Afuah (2017) offer a comprehensive account of the key reasons for studying business models. First, business models are instrumental for strategy and competitiveness.

Second, business models embody a new dimension that complements the traditional foci of innovation, i.e., product, process, organization. Third, macro-level changes in the business landscape are blurring the boundaries between formerly distinct industries, and companies are under pressure to rethink the ways of achieving their desired outcomes. This is only evidenced by the expanding body of work carried out by scholars who tap into the increasingly topical field of ecosystems (e.g., Moore, 1993; Iansiti and Levinen, 2004; Adner, 2017; Senyo, Liu and Effah, 2019; Kohtamäki, Parida, Oghazi, Gebauer and Baines, 2019; Jacobides, 2019). Fourth, as explored in the further sections, the business model perspective allows organizations to align their economic interests with the creation of environmental and/or social value, while enabling the researchers to utilize the discussed concept for exploring such angle holistically.

During the last decade, several global economic and financial crises have highlighted the impact of companies on society, leading to calls for revisiting the relationship between business and sustainable development as defined more than thirty years ago, i.e., "development that meets the needs of the present without compromising the ability of future generations to meet their own needs" (World Commission on Environmental Development, 1987, p. 41). Although the sustainability and green growth policy agenda is evident (Aagaard, 2019; Beltramello, Haie-Fayle and Pilat, 2013), there is also a realization that technology innovation alone cannot resolve all of our sustainability issues (Wells, 2013). Hence, building on Teece's (2010) seminal definition and a literature review by Boons and Lüdeke-Freund (2013), Schaltegger, Hansen and Lüdeke-Freund (2016) came up with a concept of business model for sustainability and defined it thusly: "[a] business model for sustainability helps describing, analysing, managing, and communicating (i) a company's sustainable value proposition to its customers, and all other stakeholders, (ii) how it creates and delivers this value, (iii) and how it captures economic value while maintaining or regenerating natural, social, and economic capital beyond its organizational boundaries (p. 6)."

Conventionally, value creation has predominantly been considered in terms of product or service bundles offered to customers in order satisfy their needs, or in relation to economic value created for the business in question. In the vein of the frequently referenced triple bottom line approach by Elkington (2004), the business models for sustainability broaden the scope of the field by emphasizing the social and ecological aspects of value creation in connection to stakeholders that lie outside the narrowly bounded scope of parties directly involved in the key processes and activities. Moving beyond the commonly maintained orientation toward customer-centric value proposition and pointing out the lack of research in the area of stakeholder relationships in value creation, Freudenreich, Lüdeke-Freund and Schaltegger (2020) expand the conventional one-directional understanding of value creation by exploring it from the stakeholder theory perspective, which considers business "a set of relationships among groups which have a stake in the activities that make [it] up" (Freeman, 2010, p. 7). The authors hence highlight the importance a joint purpose around which a business is built and argue mutually beneficial value creation, i.e., with the stakeholders as well as for them. The stakeholder approach is especially resonant in the context of sustainability management, as elaborately discussed by Hörisch, Freeman and Schaltegger (2014). Firstly, both perspectives explore business beyond the limited ego-centric focus on creating value only for the customer and the company itself. Acknowledging broader societal and natural embeddedness of businesses, they both reject separating business and ethics, hence condemning various forms of philanthropy, unless the value creation that leads to the resources distributed is sustainable and responsible by design. Followingly, they both resolutely oppose the thesis that profit is immoral, but also expand the short-term business outlook by seeking for value creation in a long-term horizon, especially in terms of financial, societal, and/or natural considerations, which connect them to the domain of strategic management. The key higher-level argument is that business and ethics are interrelated and inseparable. Asserting relationships and joint purpose as the key elements of business models, Freudenreich et al. (2020) hence developed a stakeholder value creation framework that diverges from the classical customer value proposition view by considering not only what is the value and how is it created, but also with and for whom. This framework distinguishes between five interdependent stakeholder groups (i.e., customers, business partners, employees, societal stakeholders, and financial stakeholders) and explicitly considers the value flows that take place in their relationships. Given the presumption that value creation occurs between multiple different actors, it is necessary to view the outcome of the process as a portfolio. Naturally, this contribution has significant implications for the discussed concept of business models for sustainability, manifested through four theoretical propositions. Firstly, the identification and solving of sustainability issues as a part of value creation processes involve all relevant stakeholders (Stubbs and Cocklin, 2008; Aagaard and Ritzén, 2020). Secondly, how the particular stakeholders contribute to achieve the business model's joint purpose, which is oriented toward sustainable development, is clearly formulated (Bocken, Short, Rana and Evans, 2014; Lüdeke-Freund and Dembek 2017; Schaltegger, Hörisch and Freman, 2017; Upward and Jones, 2015) Thirdly, the interests of the stakeholders are aligned and the social, ecological, and economic value they receive is integrated (Freeman, 2010; Hörisch, Freeman and Schaltegger 2014). And finally, the value creation with and for stakeholders embodies and integrated perspective of ethical and business considerations (Freudenreich et al., 2020). Each of these propositions allows for evaluation of business models in terms of their capacity to perform in line with the business models for sustainability. While further contemplations on the topic of sustainable value creation through business models can be also found in several other outlets (e.g., Upward and Jones, 2015; Schneider and Clauß, 2019; Lüdeke-Freund, Rauter, Pedersen and Nielsen, 2020), commercialization of technological innovations while aspiring to create sustainable value with and for stakeholders entails a number of barriers. For instance, besides appropriability regime, complementary assets, discursive ambiguity, directional risks, methodological constraints or issues with double externality, the list also includes unsustainable dominant designs which can be changed only by radical innovation and interventions of system-level scale (Teece, 1986; Boons, Montalvo, Quist and Wagner, 2013; Lüdeke-Freund, 2020).

As Lüdeke-Freund (2020) argues, the knowledge about what prevents sustainable value creation is "extensive but not yet conlusive" and requires further insight. For instance, Brem and Puente-Díaz (2020) highlight that "[the] social dimension of sustainability has not received the same amount of attention as environmental or economic sustainability. Hence, the construct of social sustainability lacks conceptual and operational clarity (p. 4)." While the field is still in its nascent stage, the body of literature on socially sustainable business is growing and offers a "huge scope and impetus for future scholarly works" (Soni, Mangla, Singh, Dey and Dora, 2021). At the same time, however, it is crucial to point out that although business model literature acknowledges the importance of the social side of sustainability, it basically overlooks that in the interconnected world which essentially relies on flows of data and information, one simply cannot discuss sustainability without involving privacy as well as its protection. The following sections hence introduce privacy as a major social issue within the stream of sustainability focused business model research and suggest how to tackle it.

The Role of Privacy in Business Development

Establishing the interdisciplinarity between the domains of business model and sustainability allows to shift focus to a gently smouldering platform that is about to burst into flames—a highly interrelated and far-reaching issue of privacy.

The quest for discovering how to jointly propose, create, deliver, and capture value while protecting privacy have not only had a prominent spot in the research agendas of scholars running the academic gamut from engineering to philosophy. It has also been raison d'être for some of the key public, private and non-profit institutions. According to the OECD Digital Economy Outlook 2020 report (2020), the absolute majority of OECD member countries consider the main challenge to their privacy and data protection regulatory frameworks to be catching up with the technological developments and business models of online platforms. What is more, in order to prevent their value creation from being hampered, the digital platforms have been even encouraged to self-regulate (Cusumano, Gawer and Yoffie, 2021). Ultimately, more than 80 percent of the countries consider artificial intelligence (AI) and big data to pose the main challenge for privacy and personal data protection. These findings are also very much in line with further global projections, which consider privacy to be one of the great tensions of the coming years (Reinsel, Rydning and Gantz, 2020).

To explain the reasons behind such an upset, in the words of Montes and Goertzel, AI space is essentially "dominated by an oligopoly of centralized mega-corporations (2019, p. 354)" that expand into an increasing number of verticals. Such actors seemingly enhance privacy at the cost of creating bottlenecks, raise barriers to entry, and strengthen their position as ecosystem orchestrators controlling majority of the core society-wide operations. Looking under the proverbial hood of these hyperscalers, it can be seen that compared to the traditional operating models that rely predominantly on the processing power of employees, the value creation capacity of enterprises centring their business models around AI becomes far superior. In this environment, differentiation takes place through finding a right position within particular ecosystems and integrating algorithms into the very core of value creation processes. As Iansiti and Lakhani (2020a) point out, due to the push for constant innovation and improvement, we witness that companies holistically embracing the potential of algorithms can be scaled up at a faster pace, allowing for much broader scope and create unprecedented learning opportunities. Although having more data and information does not necessarily equal higher competitive advantage, through a thorough consideration and careful cultural alignment, companies can create network effects that enable almost exponential and long-lasting value creation without diminishing returns (Hagiu and Wright, 2020).

These disruptive changes are naturally followed by consequences of the same magnitude. Besides other factors, the performance of AI depends extensively on the nature, type and volume of data and associated information – including the circumstances and conditions under which they were collected. The consent-based rules of the game are notoriously ill-suited to tackle the social challenges, as they only nurture trading data and information for a particular outcome in a quid pro quo fashion, or in other words, in the vein of the so called "privacy paradox," i.e., the flawed logic of a phenomenon where people say they highly value privacy, and subsequently decide not to protect it, or even voluntarily exchange it for goods and services of inadequate value (Solove, 2020; Berinato, 2018). The concern of people over exploitation of their personal data generally differs (e.g., Cecere, Le Guel and Soulié, 2015) and, to cite Acquisti et al., "consumers' ability to make informed decisions about their privacy is severely hindered because consumers are often in a position of imperfect or asymmetric information regarding when their data is collected, for what purposes, and with what consequences" (2016, p. 442). Thus, in digital economies where data and information are aggregated, combined, and distributed across ecosystems, informing individuals and empowering them with higher control while calling for firms to be transparent about their practices not only does not result in privacy being protected – in a number of cases, it can also backfire (Acquisti, Brandimarte and Loewenstein, 2015).

As can be summarized by using citation from a recent World Health Organization report reflecting on the sustainability of AI in healthcare "[the] pursuit of data, whether by government or companies, could undermine privacy and autonomy at the service of government or private surveillance or commercial profit. (p. 2, 2021)". While the regulators have been indefatigably attempting to curb the power of the key industry-shaping players, their efforts have not been particularly effective (e.g., Jacobides, Bruncko and Langen, 2020). To cite Véliz, "digital technologies can only constitute progress if they serve the well-being of citizens and the flourishing of democracy" (2021, p. 11). Many have discussed that a threat to privacy means a direct threat to democratic principles (e.g., Gavison, 1980; Simitis, 1987; Regan, 1995; Reiman, 1995; Roessler, 2005; Lever, 2006; Goold, 2009; Hughes, 2015; Richards, 2015); however, nowadays, individuals as well as organizations have basically two options – get locked-in into the prevalent business models or reconcile with their demise as a functioning part of the society. Based on the ongoing developments, it is reasonable to assume that until creating superior value requires exploitation of personal information, doing so will remain to be a justifiable modus operandi. At the same time, as long as protecting privacy remains understood as contradicting the idea of creating value through leveraging network effects, modularity and complementarity, it will remain a niche endeavour of seemingly utopistic enthusiasts struggling to scale their ventures to the level of economically self-sufficient business cases.

Understanding Privacy as a Social Value

In 1945, after the end of World War II, the United Nations was founded. Three years later, its General Assembly set forth the Universal Declaration of Human Rights as a "common standard of achievements for all peoples and all nations." In Article 12, the Declaration recognized that "no one shall be subjected to arbitrary interference with [her] privacy, family, home or correspondence, nor to attacks upon [her] honour and reputation" and that "everyone has the right to the protection of the law against such interference or attacks." Privacy thus became one of the fundamental human rights (United Nations, 1945, 1948). Although the core focus of this paper does not allow for discussing the full background of the originally predominant liberal perception of privacy rooted in Warren and Brandeis (1890), shaped by Prosser (1960), Westin (1967), or Roessler (2005), it is critical to mention that the perception on privacy has always reflected the major societal changes (Keulen and Kroeze, 2018). Notably, to illustrate, the diminution of printing regulations in 18th-century England resulted in the upheaval of newspapers and the rise of the first indications of celebrity culture. Trading private life as a public commodity has led to further efforts to separate private and public personae, establishing the archetypal link between privacy and technology (Fawcett, 2016).

According to Margulis (2003), the understanding of privacy has been significantly influenced by the work of Altman. Defining privacy as "the selective control of access to the self" (1975, p. 24), Altman proposes that privacy has five properties. First, privacy is a temporal dynamic process of controlling the interpersonal boundaries, regulating interaction with others through determining how open or closed a person is in response to changes in their internal states and external conditions. Second, there is a difference between the desired and actual levels of privacy. Third, privacy is non-monotonic, meaning that the optimal level of privacy is achieved when the actual level of privacy corresponds to the desired, creating the possibility of too much privacy in cases when the actual level of privacy is higher than desired (e.g., social isolation) and the possibility of too little privacy in cases when the actual level of privacy is lower that desired (e.g., crowds). Fourth, the nature of privacy is bi-directional and entail inputs from others (e.g., noise) and outputs to others (e.g., oral communication). Finally, there are two levels of analysis at which privacy applies, i.e., individual level as well as group level.

Altman's contribution rooted in projecting privacy as an inherently social process has challenged the liberal view on privacy revolving around autonomy as social detachment. As argued by Mokrosinska (2018), "saying that privacy protects autonomy is to say that privacy also protects the practices in which the agent exercises her autonomy" (p. 123); therefore, one cannot discuss the privacy of an individual, without the privacy of her social relations. In addition, building on the relational perspective maintained by Fried (1968) and Rachels (1975), Roessler and Mokrosinska (2013) further argue that privacy not only regulates and facilitates the "social conditions of the meaningful exercise of autonomy" (p. 779) but that it also constitutes the social relations as a condition of autonomy. This, in essence, means that a threat to privacy is a threat to society as such.

The focus on autonomy, control, and right of an individual has notably shifted toward a broader social value, not coincidentally in parallel with the development of some pivotal technologies, including the invention and commercial application of microprocessors in 1971 (Intel, 2020), transition of the ARPANET host protocol from NCP to TCP/IP (i.e., birth of Internet) in 1983 (Leiner, Cerf, Clark, Kahn, Kleinrock, Lynch, Postel, Roberts and Wolff, 1997), and the launch of the World Wide Web in 1993 (CERN, 2020). Scholars, including Friedrich (1971), Simmel (1971), Thomson (1975), Scanlon (1975) and Rachels (1975), started to recognize the social value of privacy and, to cite Simitis (1987), who reviewed the concept of privacy in in the context of information society, it was necessary to move away from discussing privacy as a "tolerated contradiction" of the right to be let alone and the need to be informed, toward understanding it as a "constitutive element of a democratic society" (p. 732).

Along these lines, arguing that privacy is not only of value to individuals but to society in general as well, Regan (1995) proposed three bases for the social importance of privacy. First, on the basis of Mill (1863), Gavison (1980), and data-evidenced public opinion, Regan (1995) proposes that privacy is a common value as it is valued by all individuals and all individuals share some perceptions about it. Second, reflecting on the importance of privacy to the democratic political process (e.g., targeting political messages through the exploitation of personal information), Regan defines privacy as a public value. And third, considering that market forces and technology make it hard for an individual to have privacy without all individuals having similar minimum level of privacy, she regards privacy as a collective value. Furthermore, drawing on Coase's paper "The Lighthouse in Economics" (1974), Regan presents three key reasons why privacy can virtually be considered a "collective or public good" (Regan, 2018, p. 59). Firstly, due to the non-voluntary nature of record-keeping in various relationships, one cannot simply acquire or establish privacy to the level that is desired. The cost of unwillingness to take part in essential relationships (e.g., healthcare, education, or banking) for the sake of protecting privacy would lead to serious issues on the individual as well as societal level. Secondly, market is an inefficient mechanism for supplying an optimal supply of privacy. Regan states that privacy choices are often hidden transaction costs and considers privacy invasions to be the result of market failures. Furthermore, she argues that in this matter, privacy is in fact similar to clean air or national defence. Thirdly, the interrelatedness and complexity of the communication infrastructures increases the difficulty of dividing privacy. In other words, the design of the technology that enables the communication to take place determines the level of privacy possible to be achieved. As Regan concludes, "if we did recognize the collective or public-good value of privacy, as well as the common and public value of privacy, those advocating privacy protections would have a stronger basis upon which to argue for its protection" (Regan, 1995, p. 231).

A related issue of fundamental importance is discussed by Solove, who denies the possibility of articulating the meaning privacy at all, calling it a "concept of disarray" that among other things encompasses "freedom of thought, control over one's body, solitude in one's home, control over personal information, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations" (Solove, 2008, p. 1). Asserting that privacy "consists of many different yet related things" (Solove, 2008, p. 9), he suggests that the traditional way of conceptualizing privacy should be abandoned for an approach based on Wittgenstein's philosophical idea of family resemblance, i.e., concepts drawing from a common pool of similar elements rather than having a single common characteristic. Solove argues that the nature of privacy and its social value is pluralistic and highly dependent on its context (2015) and further points out a key discourse concerning the trade-off between privacy and security where "privacy often loses to security where it shouldn't" (2011, p. 2). He proposes that people are encouraged to accept that in order to be more secure, they need to sacrifice their privacy. This presumption is also widely present in management literature. For instance, Casadesus-Masanell and Hervas-Drane emphasize that trading off privacy for use of various "information-sensitive" services are "defining business models and the role of privacy in online marketplaces" (2015, p. 229). Building on this article, the authors recently developed a framework that helps firms that accumulate and exploit personal information to manage privacy, i.e., delivering the benefits while mitigating the threats (Casadesus-Masanell and Hervas-Drane, 2020). This firm-centric roadmap divides privacy landscape into four domains and corresponding external players: government (political environment); hackers (security environment); third parties (market environment);

and peers (social environment). They argue that on the one hand, disclosure allows companies to tap into new revenue streams and can be profitable and desirable when generating positive impact to consumers. On the other, it can be also harmful as it "generates distraction, distress, or detrimental consequences (such as higher prices)" (p. 8). The authors suggest that this "conflict of interest" can be resolved by compensating consumers for disclosure, limiting disclosure and sacrifice revenues, or in the worst case ceasing the disclosure altogether (p. 8).

In this article, however, such logic is challenged. Approaches built on refining the mechanisms of control and access only feed the faulty perception that giving up privacy is necessary (and sometimes even reasonable) if the consumers "name the price" for such a practice. Not only that individuals assign markedly different values to the privacy of their data, their assumptions are also based on different factors, and the market to trade data in a fair way does not exist (Acquisti, John and Loewenstein, 2013). The rationale upon which such imbalanced deliberations stand is per se based on misleading views about the understanding of privacy protection, its costs, and benefits, which resultingly lead to unfair, inadequate, and unnecessarily skewed compromises at the expense social well-being (Solove, 2011; Acquisti et al., 2016). Building our digital future on a principle that wrongdoing can be justified by a certain amount of money sets a dangerous precedent that one can buy a privilege to exploit others, hence undermines the very core idea of egalitarianism. People cannot avoid sharing data and information, the question is how to do that in a way that is sustainable for everyone – individual, society, as well as companies.

Privacy and Contextual Integrity

Protecting personal data against sharing can have both positive and negative effects on societal and individual welfare (Acquisti et al., 2016). According to the highly influential and thoroughly developed theory of contextual integrity by Nissenbaum (2010), protecting privacy is not about restricting the flow of information or ensuring the right to control it. Opposing the ineffective procedural approaches (e.g., informed consent practice) rooted in the five fair information practice principles coined by US Secretary's Advisory Committee on Automated Personal Data Systems (U.S. Department of Health, 1973), Nissenbaum (2011) argues that "notice-and-consent, however refined, will [not] result in better privacy online as long as it remains a procedural mechanism divorced from the particularities of relevant online activity" (p. 35). She suggests that the pivotal rationale lies in making the flow of the personal information appropriate. The appropriate flow of information is, in essence, defined by its conformity with entrenched social norms that meet the context-relative expectations. Therefore, when the flow of information conforms with the norms, it can be considered appropriate, hence privacy can be deemed preserved. In short, the information norms are constructed by three independent parameters whose value must be specified in order to allow for determining whether an information flow is appropriate, i.e., conforming the context-specific social domain. These parameters are actors (i.e., subject, sender, recipient), attributes (i.e., information types), and transmission principles. When identifying actors, it is necessary to identify their contextual roles "to the extent possible," i.e., "capacities in which each are acting" (Nissenbaum, 2010, p. 141). Followingly, attributes describe the nature of information in question, i.e., "kind and degree of knowledge" (Rachels, 1975, p. 71). Finally, the parameter of transmission principle is embodied in particular terms and conditions under which the transfer of information should or should not happen (e.g., confidentiality). In order to operationalize the descriptive framework, Nissenbaum further also offer a nine-step augmented contextual integrity decision heuristic adapted for situations where nonconforming practices outperform the entrenched norms (Nissenbaum, 2010, pp. 181–182):

1. *Describe the new practice in terms of information flows.*
2. *Identify the prevailing context. Establish context at a familiar level of generality (e.g., "healthcare") and identify potential impacts from contexts nested within it, such as "teaching hospital."*
3. *Identify information subjects, senders, and recipients.*
4. *Identify transmission principles.*

5. *Locate applicable entrenched informational norms and identify significant points of departure.*
6. *Prima facie assessment*
7. *Evaluation I ...*
8. *Evaluation II ...*
9. *On the basis of these findings, contextual integrity recommends in favor of or against systems or practices under study.*

The suitedness of this theory for the digital economy as well as its potential to guide further regulatory steps is often emphasized. This can be for instance evidenced by its influence on the Privacy Bill of Rights presented by the Obama administration (The White House, 2012), which recognized "Respect for Context," as consumers' "right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data." Such a contested definition, however, opened door for various biased interpretations that could be misused for the benefit of the affected incumbents. In her response, Nissenbaum (2015) argued that one of the key issues emerged from the related discourse is understanding context as business model. Asserting that it "offers no prospect of advancement beyond the present state-of-affairs" as "its proponents seem to expect individuals and regulators to sign a blank check to businesses, in collection, use, and disclosure of information based on exigencies of individual businesses," she suggests that respecting context as social domain equals "to respect contextual integrity, and, in turn, to respect information norms that promote general ethical and political values, as well as context specific ends, purposes, and values" (p. 848).

Although this argument is very much in line with the theories that focus on sustainability research, this article argues that for the contextual integrity to be suitable for viable and feasible application in a social domain where a transmission of data and information plays any role in the process of value proposition, creation, delivery, and capture, one necessarily needs to consider the use of the data and calibrate it with respect to the social domain as well. As previously mentioned, nowadays, we witness self-interested companies with varying degrees of multilateral non-generic complementarities being interdependently embedded in non-hierarchical structures and jointly creating value through redefined business models adapted for exponential data-driven growth (Jacobides et al., 2018; Bogers, Sims and West, 2019; Iansiti and Lakhani, 2020b). Therefore, in the environment that consists of ecosystems, the assumption that the contextual role of an actor is bounded, defined, and fixed is no longer valid. An actor can have multiple roles in multiple contexts and can use the data and information in multiple, non-contextual ways. Even data aggregates can ultimately result in far-reaching impacts on individuals as well as society. Moreover, when actors A and B both individually transmit data and information in conformity with contextual integrity, the conformity cannot be guaranteed if these actors combine and/or accumulate the data and information, for instance for the purposes of value proposition, creation, delivery, and capture. Based on that, it is necessary to argue that a business model which is based on transmission of data and information cannot be considered sustainable if it does not function in compliance with contextual integrity, while contextual integrity cannot be considered applicable in business environment unless the use of data is considered. This proposition is hence elaborated in the following section.

Mutual Embeddedness of Contextual Integrity and Business Models for Sustainability

As manifested by the stream coined business models for sustainability (Schaltegger et al., 2016), the relation between business models and sustainability has received an increasing amount of scholarly attention. With the almost exponential rise of information technologies, we have been experiencing since the 1970s, the issue of protecting privacy as a social value has increased in importance and popularity, especially in the areas of technology and philosophy. Considering the current state of global affairs, the most suited approach to privacy protection can be considered the theory of contextual integrity (Nissenbaum, 2010). Synthesizing the two so far siloed but mutually relevant theories, this article posits

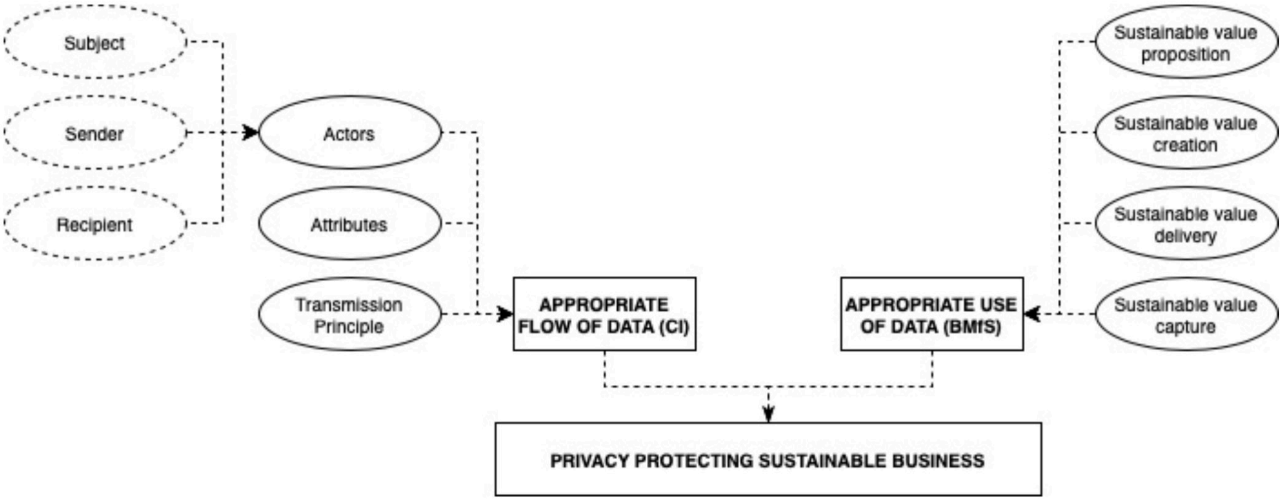
Subject
Sender
Recipient
Actors
Attributes
Transmission Principle
APPROPRIATE FLOW OF DATA (CI)
APPROPRIATE USE OF DATA (BMfS)
Sustainable value proposition
Sustainable value creation
Sustainable value delivery
Sustainable value capture
PRIVACY PROTECTING SUSTAINABLE BUSINESS

Figure 1: Business models for sustainability and contextual integrity – schema of synthesis

that businesses which protect privacy in a sustainable way have to treat privacy as a social value constituted by two key elements, i.e., appropriate flow of data and information and appropriate use of data and information. While appropriate flow of data and information is rigorously addressed by the theory of contextual integrity, the appropriate use of data and information by businesses can be addressed by the theory of business models for sustainability. The suggested synthesis is schematically demonstrated in Figure 1.

Based on this assumption, there needs to be a close, proactive interplay between the prescriptive elements of the theories mentioned above. Therefore, on the basis of the augmented contextual integrity decision heuristic and the business models for sustainability assessment questions stemming from the stakeholder value creation framework, a heuristic framework for privacy and sustainability in business models has been developed. This framework consists of a foundational dimension that facilitates mapping of the necessary indicators of privacy in business models for sustainability, followed by an assessment dimension comprising evaluation principles lined up in a continuum. The core purpose of this theoretical framework is to suggest a system of key considerations that needs to be in place when assessing whether a particular business practice sustainably protect privacy. The framework is illustrated in Figure 2 and the considerations further elaborated in the following sections.

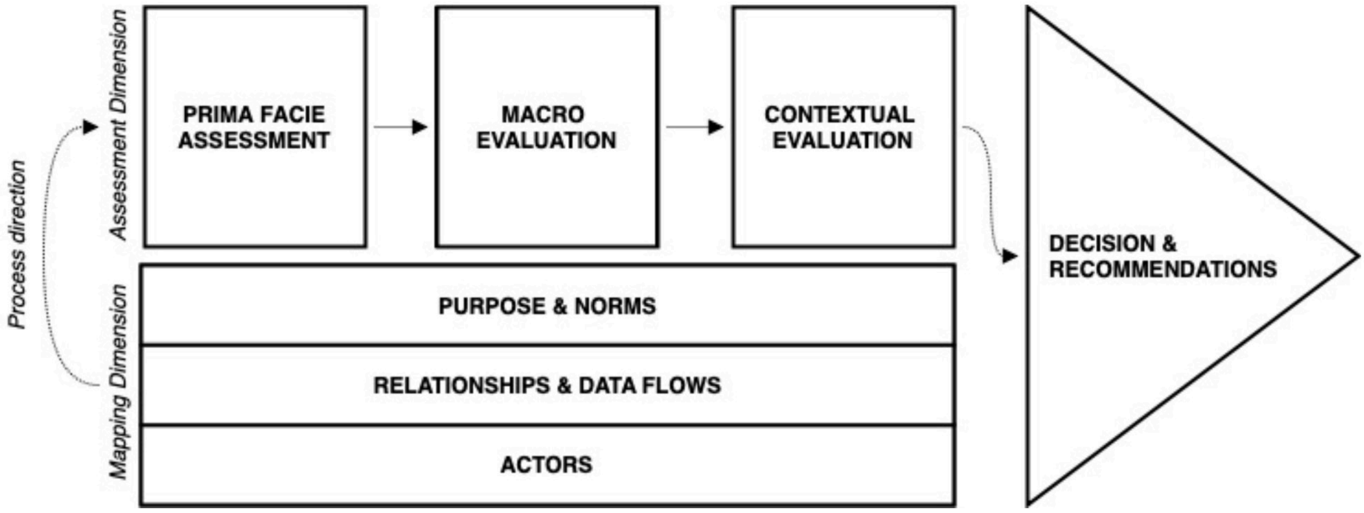

Figure 2: Heuristic framework for privacy and sustainability in business models

Mapping Dimension Components

Actors

In exploring the area of actors, first, there is a need to determine the boundaries of the context in question. Furthermore, it is also important to explore its sub-contexts and their potential impacts on that very context (Nissenbaum, 2010). Companies operating in different contexts interact with a number of distinct stakeholders that play particular roles in value creation as well as in the transmission of data and information for doing so (Adner, 2017; Jacobides et al., 2018; Bogers et al., 2019; Iansiti and Lakhani, 2020b). For that reason, it is not only necessary to distinguish between employees, customers, business partners, financial stakeholders, and societal stakeholders (and possibly also other relevant stakeholders) (Stubbs and Cocklin, 2008; Aagaard and Ritzén, 2020; Freudenreich et al., 2020). It is equally important to determine what is the nature of the information in transmission (Rachels, 1975) who is sending the data and information, who is the subject, and who is the recipient of the data and information (Nissenbaum, 2010). Most probably, the interests and expectations of these stakeholders might differ (Freeman, Pierce and Dodd, 2000). Thus, it is crucial to determine to what extent their interests are in collision or alignment and what the resulting implications or risks for the overall outcome could be (Freeman, 2010; Hörisch et al., 2014; Patala, Jalkala, Keränen, Väisänen, Tuominen and Soukka, 2016).

Relationships and Data Flows

Besides identifying the key actors, it is equally important to specify the flows of data and information that take place between them as the business model is being operationalized (Nissenbaum, 2010). These flows should be in line with the core principles of the business models for sustainability, i.e., adjusted in a way that pro-actively contributes creating to social, economic, and potentially also ecological value (Schaltegger et al., 2016). It is also required to determine the interests and vulnerabilities of the particular entities, who co-creates what value with whom, and who the recipient of the particular value is (Freudenreich et al., 2020). Furthermore, it is important to carefully consider the terms and conditions under which the transmission of data and information ought (and ought not) to happen (Nissenbaum, 2010). This principle must be in line with the contextual norms of the particular social domain and clearly understood by all the stakeholders. It is necessary to understand that in order to protect privacy in a sustainable way, the business model must be by design compliant with contextual integrity. Therefore, even if a person gives an explicit permission to the business to sell her data and information to a third party, if a social domain is not respected, the business should be considered neither sustainable nor protecting privacy.

Purpose and Norms

In order to be able to see whether a business model is protecting privacy, it is necessary to identify the entrenched norms of the particular social domain (Nissenbaum, 2010). Besides that, it must be explored whether the business model of interest provides sufficient foundations for the stakeholders to co-create value without violating these norms. Since the value operations are being carried out in an interrelated manner, it is pivotal to determine the joint purpose of all the involved actors and whether the purpose is directed toward creating a sustainable value (Bocken et al., 2014; Lüdeke-Freund and Dembek 2017; Schaltegger et al., 2017; Upward and Jones, 2015). Importantly, the focus should be on the actual actions and real contributions toward sustainability. Ultimately, it is necessary to explicitly specify what the joint purpose is and how it helps to achieve a particular sustainable development goal in a contextually appropriate way (Nissenbaum, 2010, Stubbs and Cocklin 2008).

Assessment Dimension Components

Prima Facie Assessment

After identifying the key components of the framework, it is necessary to evaluate the dynamic aspects of the business model, i.e., the operationalization of value-related activities in relation to the identified entrenched norms and joint purpose. The goal of the prima facie assessment is to determine whether the business model in question involves major discrepancies that would reveal its insufficiency straight away. This step involves making sure that all of the components are mapped to the fullest extent possible and determining whether they raise any issues by themselves. Are the data and information flows used for operationalization of the business model in line with entrenched norms? If not, does the business model have an innovation potential which could result in a significant sustainable improvement of the status quo? Does the business model have the capacity to facilitate the relationships that jointly create value in line with sustainability principles? Are the relationships ethical, respectful, and fair? If the business model is found to be in contradiction with the basic principles of the framework, it can be deemed unsatisfactory to comply with the idea of sustainable privacy protection in business as such. Finally, it is also crucial to consider that business models designed or innovated to exploit a new technology, i.e., AI, might operate in an environment where no norms have been established yet. In such cases, the business model cannot be rejected prima facie, and can, therefore, be subjected to the next step of evaluation.

Macro Evaluation

The second step of the assessment part is evaluation of social, economic, and environmental macro factors affected by the business model. Besides considering whether the business model could harm autonomy and freedom (i.e., what is its effect on power structures within society, what are its implications for social hierarchy, justice, fairness, democracy, equality, and other factors pointed out by the theory of contextual integrity itself), there is also a need to consider whether the actors can actually ethically exploit the appropriate flows of data and information to propose, create, deliver, and capture value with and for stakeholders while being economically prosperous without harming the environment (or even pro-actively contribute to its recovery).

Contextual Evaluation

After determining how the business model impacts the environment from the higher perspective, its concrete impacts on the particular context within which it operates should be further determined. Furthermore, as the types of value that need to be proposed vary across the spectrum of stakeholders within the context, it is important to find out whether the proposition reflects the diversity of stakeholders sufficiently. Essentially, this phase of evaluation is set to ascertain whether the business model exploits data flows in a way that impacts the ecosystem of actors in a way that threatens the sustainability of the context per se.

Decision and Recommendation

When approaching the final phase of this high-perspective heuristic framework, it should be possible to carry out a fair judgement as of whether a particular business model protects privacy while operating in line with the core principles of sustainable value proposition, creation, delivery, and capture. If the business model is not found suitable, it is important to implement changes and iterate until appropriate flow and use of data and information is achieved.

Conclusion and Discussion

This article posits that in order to operate sustainably, businesses playing any role in proposing, creating, delivering, or capturing value through transmission of data and information must approach privacy as a social value. Furthermore, they also need to protect it by ensuring that the flow and use of data and information across their ecosystems is appropriate. This means that the flow of data and information must be in line with the theory of contextual integrity (Nissenbaum, 2010), while the use of data and information must be in line with the theory of business models for sustainability (Schaltegger et al., 2016). While synthesizing these two rigorously developed streams of research, this article proposes a heuristic framework for privacy and sustainability in business models, which prescriptively operationalizes the theories in line with the augmented contextual integrity decision heuristic (Nissenbaum, 2010) and the stakeholder value creation framework (Freudenreich et al., 2020).

Firstly, this article unfolds the relevance of privacy protection for the stream of business model research directed toward sustainable development in a way that is theoretically rigorous, complementary with the stakeholder theory, and reflecting the impact of technology on business. This contributes especially to addressing the need for further research on specific sustainable value creation barriers identified by

Lüdeke-Freund (2020), as well as extends the theory of business models for sustainability (Schaltegger et al., 2016; Freudenreich et al., 2020). Secondly, the synthesis contributes to the contemporary debate on privacy as a social value, mainly through identifying theoretically thorough avenue for adapting the theory of contextual integrity (Nissenbaum, 2010) to a social domain where value proposition, creation, delivery, and capture with and for multilaterally interdependent stakeholders involves transmission of data and information.

Considering the foresight of increasing dependency on data processing, the success of cultivating the underlying fabric of our society is directly related to the effectivity of privacy protection mechanisms. Hence, from the perspective of future research, the developed framework can be especially useful for constructing narratives of how the inevitable technological progress can be leveraged in ensuring ultimate equity and inclusivity in the digitalized world. This article ultimately posits that the future of democracy in digital society leans upon the efforts to move beyond the implicit tolerance of the chokehold imposed by the omnipresent centralization (cf. Hensmans, 2021). And despite the obvious drawback residing in the lack of empirical perspective, it may be suggested that the presented contributions can be also reflected in managerial practice. First of all, based on its prescriptive nature, it shall be implied that professionals can use the heuristic framework for privacy and sustainability in business models to evaluate what elements in their business model portfolios have to be amended in order for their company to sustainably protect privacy. This proposition differs from the standalone theories especially by the fact that it postulates the mutual relationship between privacy protection and sustainability. In practice, this means that a business model that involves transmission of data and information cannot be considered sustainable unless it protects privacy.

Besides creating a stepping-stone for addressing the issue of sustainable privacy protection holistically, this synthesis also entails a number of implications. From a theoretical angle, this contribution proposes a revision of the theory of contextual integrity by considering not only the flow of the data and information but also their use. This article addresses the use by considering how value is proposed, created, delivered, and captured by an organization and its stakeholders. However, the unprecedented data-processing operations are not detectable only in cases when actors are involved in business activities. For that reason, it should be explored how the use of data and information can be addressed in cases of various backgrounds. Finally, this synthesis introduces the privacy research stream to the stream of business model literature and argues that under current circumstances escalated by the COVID-19 pandemic, there is a need for a genuine interdisciplinarity – one that builds on stable theoretical foundations rooted in diverse research domains.

This contribution is to be considered offering a vision delineating and emphasizing the privacy protection aspect for future sustainable transitions. And although this meta-perspective suffices the needs of an architect drawing up a blueprint (as mentioned in the Research Design section), it does not allow for diving deep into the particularities of the constituent fragments and implications. For that reason, the synthesis should not be challenged only theoretically but also through further empirical research, possibly investigating how businesses actually attempt to sustainably protect privacy, how privacy-centric focus impacts the business model development of companies in different ecosystems, and what role privacy plays in the business models of incumbents. Furthermore, there is a vast research potential in exploring how can companies in diverse ecosystems co-create and co-capture value through sharing data and information without compromising human-centricity. Similarly, from a different angle, a promising research avenue emerges within the realm of start-ups and entrepreneurs that put privacy protection and social values as a keystone of their existence. Based on the proposition that privacy can be only protected when a business model is economically feasible, it is important to explore how can such entities become financially stable. What are the drivers and challenges of their efforts? What are the characteristics of their ecosystems and their relationship with the previously illustrated "oligopolies"? How do they interact with incumbents when entering established ecosystems? These questions need to be explored particularly in industries where privacy protection is outweighed by a higher cause goal of immediate importance and effect, such as healthcare (e.g., Grundy, Chiu, Held, Continella, Bero and Holz, 2019; Panch, Mattie and Celi, 2019; Sharma and Bashir, 2020; Rezaei, Jafari-Sadeghi, Cao and Mahdiraji, 2021). When conducted comprehensively, by understanding the social domain as a context, these studies may have an immensely informative effect on regulations – because improving the state of society by regulating AI-based ecosystem actors using rules and sanctions that require them to revise their consent has no chance to succeed.

References

Aagaard, A. (2019). Sustainable business models—Innovation, implementation and success. London: Palgrave MacMillan.

Aagaard, A. and Rezac, F. (2022). Governing the interplay of inter-organizational relationship mechanisms in open innovation projects across ecosystems. Industrial Marketing Management, 105, 131–146.

Aagaard, A. and Ritzén, S. (2020). The critical aspects of co-creating and co-capturing sustainable value in service business models. Creativity and Innovation Management, 29(2), 292–302.

Acquisti, A. John, L. and Loewenstein, G. (2013). What is privacy worth? Journal of Legal Studies, 42(2), 249-274.

Acquisti, A., Brandimarte, L. and Loewenstein, G. (2015). Privacy and human behavior in the age of information. Science, 347(6221), 509–514.

Acquisti, A., Taylor, C. R. and Wagman, L. (2016). The economics of privacy. Journal of Economic Literature, 52(2), 1–64.

Adner, R. (2017). Ecosystem as structure: An actionable construct for strategy. Journal of Management, 43(1), 39–58.

Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, and crowding. Monterey: Brooks/Cole.

Amit, R. and Zott, C. (2012). Creating value through business model innovation. MIT Sloan Management Review, 53(3), 41–49.

Astley, W. G. and Fombrun, C. J. (1983). Collective strategy: Social ecology of organizational environments. Academy of Management Review, 8(4), 576-587.

Bansal, G., Zahedi, F. and Gefen, D. (2015). The role of privacy assurance mechanisms

in building trust and the moderating role of privacy concern. European Journal of Information Systems 24, 624–644.

Beltramello, A., Haie-Fayle, L. and Pilat, D. (2013). Why new business models matter for green growth. OECD Green Growth Papers, 2013-01, OECD Publishing, Paris.

Berinato, S. (2018). Stop Thinking About Consent: It Isn't Possible and It Isn't Right. Harvard Business School Cases, 2965. Retrieved from Harvard Business Review: https://hbr.org/2018/09/stop-thinking-about-consent-it-isnt-possible-and-it-isnt-right

Bocken, N., Short, S., Rana, P. and Evans, S. (2014). A literature and practice review to develop sustainable business model archetypes. Journal of Cleaner Production, 65, 42–56.

Bogers, M., Sims, J. and West, J. (2019). What is an ecosystem? Incorporating 25 years of ecosystem research. Academy of Management Proceedings, 2019(1), 1–29.

Boons, F. and Lüdeke-Freund, F. (2013). Business models for sustainable innovation: State-of-the-art and steps towards a research agenda. Journal of Cleaner Production, 45, 9–19.

Boons, F., Montalvo, C., Quist, J. and Wagner, M. (2013). Sustainable innovation, business models and economic performance: An overview. Journal of Cleaner Production, 45, 1–8.

Brem, A. and Puente-Díaz, R. (2020). Are you acting sustainably in your daily practice? Introduction of the Four-S model of sustainability. Journal of Cleaner Production, 267, 122074.

Burt, A. (2018, October 23). Why privacy regulations don't always do what they're meant to. Retrieved from Harvard Business Review: https://hbr.org/2018/10/why-privacy-regulations-dont-always-do-what-theyre-meant-to

Burt, A. (2019, January 03). Privacy and cybersecurity are converging. Here's why that matters for people and for companies. Retrieved from Harvard Business Review: https://hbr.org/2019/01/privacy-and-cybersecurity-are-converging-heres-why-that-matters-for-people-and-for-companies

Caputo, A., Pizzi, S., Pellegrini, M.M. and Dabić, M. (2021). Digitalization and business models: Where are we going? A science map of the field. Journal of Business Research, 123(2021), 489–501.

Casadesus-Masanell, R. and Hervas-Drane, A. (2020). Strategies for managing the privacy landscape. Long Range Planning, 53(4), 101949.

Casadesus-Masanell, R. and Hervas-Drane, A. (2015). Competing with privacy. Management Science, 61(1), 229–246.

Cecere, G., Le Guel, F., Soulié, N. (2015). Perceived Internet privacy concerns on social networks in Europe. Technological Forecasting and Social Change, 96, 277–287.

CERN. (2020). The birth of the Web. Retrieved from https://home.cern/science/computing/birth-web

Chesbrough, H. (2010). Business model innovation: Opportunities and barriers. Long Range Planning, 43(2–3), 354–363.

Cisco. (2020, March 9). Cisco Annual Internet Report (2018–2023) White Paper. Retrieved from https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Cloarec, J. (2020). The personalization–privacy paradox in the attention economy. Technological Forecasting and Social Change, 161, 120299.

Coase, R. H. (1974). The lighthouse in economics. Journal of Law and Economics, 17(2), 357–376.

Cochrane, K. (2018, June 13). To regain consumers' trust, marketers need transparent data practices. Retrieved from Harvard Business Review: https://hbr.org/2018/06/to-regain-consumers-trust-marketers-need-transparent-data-practices

Cropanzano, R. (2009). Writing nonempirical articles for Journal of Management: General thoughts and suggestions. Journal of Management, 35(6), 1304–1311.

Cusumano, M. A., Gawer, A. and Yoffie, D. B. (2021, January 15). Social media companies should self-regulate. Now. Retrieved from Harvard Business Review: https://hbr.org/2021/01/social-media-companies-should-self-regulate-now

DaSilva, C. M. and Trkman, P. (2014). Business model: What it is and what it is not. Long Range Planning, 47(6), 379–389.

Desai, V., Fountaine, T. and Rowshankish, K. (2022). A Better Way to Put Your Data to Work. Harvard Business Review, 100(4), 100–107.

Elder, L. and Paul, R. (2009). A glossary of critical thinking terms of concepts: The critical analytic vocabulary of the English language. Dillon Beach, CA: Foundation for Critical Thinking.

Elkington, J. (2004). Enter the triple bottom line. In A. Henriques and J. Richardson (Eds.), The triple bottom line: Does it all add up? (pp. 1–16). Oxon: Earthscan.

Esteve, A. (2017). The business of personal data: Google, Facebook, and privacy issues in the EU and the USA. International Data Privacy Law, 7(1), 36–47.

Fawcett, J. (2016). Spectacular disappearances: Celebrity and privacy, 1696–1801. Ann Arbor, MI: University of Michigan Press.

Freeman, R. E., Pierce, J. and Dodd, R. H. (2000). Environmentalism and the new logic of business: How firms can be profitable and leave our children a living planet. Oxford: Oxford University Press.

Freeman, E. R. (2010). Managing for stakeholders: Trade-offs or value creation. Journal of Business Ethics, 96, 7–9.

Freudenreich, B., Lüdeke-Freund, F. and Schaltegger, S. (2020). A stakeholder theory perspective on business models: Value creation for sustainability. Journal of Business Ethics, 166, 3–18.

Fried, C. (1968). Privacy. The Yale, 77(3), 475–493.

Friedrich, C. J. (1971). Secrecy versus privacy: The democratic dilemma. In R. J. Pennock and J. W. Chapman (Eds.), Privacy and personality (pp. 105–120). New York: Routledge.

Fuller, J., Jacobides, M. G. and Reeves, M. (2019). J. Fuller, M.G. Myths and Realities of Ecosystems, MIT Sloan Management Review, 60(3), 1–9.

Gavison, R. (1980). Privacy and the limits of law. The Yale Law Journal, 89(3), 421–471.

Gilson, L. L. and Goldberg, C. B. (2015). Editors' comment: So, what is a conceptual paper? Group and Organization Management, 40(2), 127–130.

Gnyawali, D. R. and Charleton, T. R. (2018). Nuances in the interplay of competition and cooperation: Towards a theory of coopetition. Journal of Management, 44(7), 2511–2534.

Goold, B. (2009). Surveillance and the Political Value of Privacy. Amsterdam Law Forum, 1(2), 3–6.

Grundy Q., Chiu K., Held F., Continella, A., Bero L., Holz R. (2019). Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. BMJ, 364, l920.

Gstrein, O. J. and Beaulieu, A. (2022). How to protect privacy in a datafied society? A presentation of multiple legal and conceptual approaches. Philosophy & Technology, 3(2022).

Hagiu, A. and Wright, J. (2020). When data creates competitive advantage. Harvard Business Review, 98(1), 94–101.

Hensmans, M. (2021). Exploring the dark and bright sides of Internet democracy: Ethos-reversing and ethos-renewing digital transformation. Technological Forecasting and Social Change, 168, 120777.

Hirschheim, R. (2008). Some guidelines for the critical reviewing of conceptual papers. Journal of the Association for Information Systems, 9(8), 432–441.

Hörisch, J., Freeman, E. and Schaltegger, S. (2014). Applying stakeholder theory in sustainability management: Links, similarities, dissimilarities, and a conceptual framework. Organization and Environment, 27(4), 328–346.

Hughes, K. (2015). The social value of privacy, the value of privacy to society and human rights discourse. In B. Roessler and D. M. Mokrosinska (Eds.), Social dimensions of privacy: Interdisciplinary perspectives (pp. 403-418). Cambridge: Cambridge University Press.

Iansiti, M. and Lakhani, K. R. (2014). Digital ubiquity: How connections, sensors, and data are revolutionizing business. Harvard Business Review, 92, 90–99.

Iansiti, M. and Lakhani, K. R. (2020a). Competing in the Age of AI: How machine intelligence changes the rules of business. Harvard Business Review, 98(1), 60–67.

Iansiti, M. and Lakhani, K. R. (2020b). Competing in the Age of AI: Strategy and leadership when algorithms and networks run the world. Boston: Harvard Business Review Press.

Iansiti, M. and Levinen, R. (2004). Strategy as ecology. Harvard Business Review, 82, 68–78.

IDC. (2020, May 8). IDC's global DataSphere forecast shows continued steady growth in the creation and consumption of data. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS46286020

Intel. (2020). Announcing a new era of integrated electronics. Retrieved from https://www.intel.com/content/www/us/en/history/virtual-vault/articles/the-intel 4004.html

Jaakkola, E. (2020). Designing conceptual articles: Four approaches. AMS Review, 10, 18–26.

Jacobides, M. G. (2019). In the ecosystem economy, what's your strategy? Harvard Business Review, 97(5), 128–137.

Jacobides, M. G., Bruncko, M. and Langen, R. (2020, December 20). Regulating big tech in Europe: Why, so what, and how understanding their business models and ecosystems can make a difference. Retrieved from https://www.evolutionltd.net/post/regulating-big-tech-in-europe

Jacobides, M. G., Cennamo, C. and Gawer, A. (2018). Towards a theory of ecosystems. Strategic Management Journal, 39(8), 2255–2276.

Johnson, M. W., Christensen, C. M. and Kagermann, H. (2008). Reinventing your business model. Harvard Business Review, 87, 52–60.

Keulen, S. and Kroeze, R. (2018). Privacy from a historical perspective. In B. van der Sloot and A. de Groot (Eds.), The handbook of privacy studies (pp. 21–56). Amsterdam, Netherlands: Amsterdam University Press B.V.

Kohtamäki, M., Parida, V., Oghazi, H., Gebauer, H. and Baines, T. (2019). Digital servitization business models in ecosystems: A theory of the firm. Journal of Business Research, 104, 380–392.

Leiner, B., Cerf, V., Clark, D. D., Kahn, R., Kleinrock, L., Lynch, D., Postel, J., Roberts, L. G. and Wolff, S. (1997). Brief history of the Internet. Retrieved from https://www.internetsociety.org/wp-content/uploads/2017/09/ISOC-History-of-the-Internet_1997.pdf

Lever, A. (2006). Privacy rights and democracy: A contradiction in terms? Contemporary Political Theory, 5(2), 142–162.

Li, T. and Unger, T. (2012). Willing to pay for quality personalization? Trade-off between quality and privacy. European Journal of Information Systems, 21(6), 621–642.

Lüdeke-Freund, F. (2020). Sustainable entrepreneurship, innovation and business models: Integrative framework and propositions for future research. Business Strategy and the Environment, 29(2), 665–681.

Lüdeke-Freund, F. and Dembek, K. (2017). Sustainable business model research and practice: Emerging field or passing fancy? Journal of Cleaner Production, 168, 1668–1678.

Lüdeke-Freund, F., Rauter, R., Pedersen, E. R. and Nielsen, C. (2020). Sustainable value creation through business models: The what, the who and the how. Journal of Business Models, 8(3), 62–90.

Lukka, K. and Vinnari, E. (2014). Domain theory and method theory in management accounting research. Accounting, Auditing and Accountability Journal, 27(8), 1308–1338.

MacInnis, D. (2004). Where have all the papers gone? Reflections on the decline of conceptual articles. Association for Consumer Research Newsletter, Spring, 1–3.

MacInnis, D. J. (2011). A framework for conceptual contributions in marketing. Journal of Marketing, 75, 136–154.

Margulis, S. T. (2003). On the status and contribution of Westin's and Altman's theories of privacy. Journal of Social Issues, 59(2), 411–429.

Martin, N., Matt, C., Niebel, C. and Blind, K. (2019). How data protection regulation affects startup innovation. Information Systems Frontier, 21, 1307–1324.

Massa, L., Tucci, C. L. and Afuah, A. (2017). A critical assessment of business model research. Academy of Management Annals, 11(1), 73–104.

McAfee, A. and Brynjolfsson, E. (2012). Big data: The management revolution. Harvard Business Review, 90(10), 60–68.

Mill, J. (1863). On liberty (2nd ed.). Boston, MA: Ticknor and Fields.

Mokrosinska, D. (2018). Privacy and autonomy: On some misconceptions concerning the political dimensions of privacy. Law and Philosophy, 37, 117–143.

Montes, G.A., Goertzel, B. (2019). Distributed, decentralized, and democratized artificial intelligence. Technological Forecasting and Social Change, 141, 354–358.

Moore, J. F. (1993). Predators and prey: A new ecology of competition. Harvard Business Review, 71(3), 75–86.

Nissenbaum, H. (2010). Privacy in context: Technology, policy, and the integrity of social life. Stanford: Stanford University Press.

Nissenbaum, H. (2011). A contextual approach to privacy online. Dædalus, Fall, 32–48.

Nissenbaum, H. (2015). Respecting context to protect privacy: Why meaning matters. Science and Engineering Ethics, 24(24), 2018.

OECD. (2020). OECD digital economy outlook 2020. Paris: OECD Publishing.

Panch, T., Mattie, H. and Celi, L.A. The "inconvenient truth" about AI in healthcare. npj Digital Medicine, 2(77).

Patala, S., Jalkala, A., Keränen, J., Väisänen, S., Tuominen, V. and Soukka, R. (2016). Sustainable value propositions: Framework and implications for technology suppliers. Industrial Marketing Management, 59, 144–156.

Porter, M. and Heppelmann, J. (2014). How smart, connected products are transforming competition. Harvard Business Review, 92, 64–88.

Porter, M. and Heppelmann, J. (2015). How smart, connected products are transforming companies. Harvard Business Review, 93, 96–114.

Prosser, W. L. (1960). Privacy. California Law Review, 48(3), 383–423.

Rachels, J. (1975). Why is privacy important. Philosophy and Public Affairs, 4(4), 323–333.

Regan, P. (2018). Legislating privacy: Technology, social values, and public policy. In B. van der Sloot and A. de Groot (Eds.), The handbook of privacy studies (pp. 57–61). Amsterdam: Amsterdam University Press.

Regan, P. M. (1995). Legislating privacy: Technology, social values, and public policy. Chapel Hill: The University of North Carolina Press.

Reiman, J. (1995). Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. Santa Clara High Technology Law Journal, 11(1), 27–44.

Reinsel, D., Rydning, J. and Gantz, J. F. (2020). Worldwide global DataSphere forecast, 2020–2024: The COVID-19 data bump and the future of data growth. Needham, MA: IDC.

Rezaei, M., Jafari-Sadeghi, V., Cao, D., Mahdiraji, H.A. (2021). Key indicators of ethical challenges in digital healthcare: A combined Delphi exploration and confirmative factor analysis approach with evidence from Khorasan province in Iran. Technological Forecasting and Social Change, 167, 120724.

Ribeiro-Navarrete, S., Saura, J.R. and Palacios-Marqués, D. (2021). Towards a new era of mass data collection: Assessing pandemic surveillance technologies to preserve user privacy. Technological Forecasting and Social Change, 167, 120681.

Richards, N. (2015). Intellectual privacy: Rethinking civil liberties in the Digital Age. Oxford: Oxford University Press.

Rigby, D. K. (2014). Digital-physical mashups. Harvard Business Review, 92(9), 84–92.

Roessler, B. (2005). The value of privacy. Cambridge: Polity Press.

Roessler, B. and Mokrosinska, D. (2013). Privacy and social interaction. Philosophy and Social Criticism, 39(8), 771–791.

Salomone, P. R. (1993). Trade secrets for crafting a conceptual article. Journal of Counseling and Development, 72(1), 73–76.

Scanlon, T. (1975). Thomson on privacy. Philosophy and Public Affairs, 4(4), 315–322.

Schaltegger, S., Hansen, E. G. and Lüdeke-Freund, F. (2016). Business models for sustainability: Origins, present research, and future avenues. Organization and Environment, 29(1), 3–10.

Schaltegger, S., Hörisch, J. and Freeman, R. E. (2017). Business cases for sustainability: A stakeholder theory perspective. Organization and Environment, 32(5), 191-212.

Schneider, S. and Clauß, T. (2019). Business models for sustainability: Choices and consequences. Organization and Environment, 33(3), 384–407.

Schwab, K. (2016). The fourth industrial revolution: What it means and how to respond. London: Portfolio.

Senyo, P. K., Liu, K. and Effah, J. (2019). Digital business ecosystem: Literature review and a framework for future research. International Journal of Information Management, 47, 52–64.

Sharma, T. and Bashir, M. (2020). Use of apps in the COVID-19 response and the loss of privacy protection. Nature Medicine, 26, 1165–1167.

Shipilov, A. and Gawer, A. (2019). Integrating research on inter-organizational networks and ecosystems. Academy of Management Annals, 14(1), 92, 121.

Simitis, S. (1987). Reviewing privacy in an information society. University of Pennsylvania Law Review, 135, 707–746.

Simmel, A. (1971). Privacy is not an isolated freedom. In J. R. Pennock and J. W. Chapman (Eds.), Privacy and personality (pp. 71–87). New York: Routledge.

Solove, D. J. (2008). Understanding privacy. London: Harvard University Press.

Solove, D. J. (2011). Nothing to hide: The false tradeoff between privacy and security. London: Yale University Press.

Cambridge: Cambridge University Press.

Solove, D. J. (2020). The Myth of Privacy Paradox. The George Washington Law Review, 89(1), pp. 1-51.

Soni, G., Mangla, S.K., Singh, P., Dey, B.L., Dora, M. (2021). Technological interventions in social business: Mapping current research and establishing future research agenda. Technological Forecasting and Social Change, 169, 120818.

Spieth, P., Schneckenberg, D. and Ricart, J. E. (2014). Business model innovation—State of the art and future challenges for the field. R&D Management, 44(3), 237–247.

Stubbs, W. and Cocklin, C. (2008). Conceptualizing a "sustainability business model." Organization and Environment, 21(2), 103–127.

Teece, D. J. (1986). Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy. Research Policy, 15(6), 285–305.

Teece, D. J. (2010). Business Models, business strategy and innovation. Long Range Planning, 43(2–3), 172–194.

Teece, D. J. (2018). Business models and dynamic capabilities. Long Range Planning, 51(1), 40–49.

The White House. (2012). Consumer data privacy in a networked world. Washington, D.C.: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy.

Thomson, J. J. (1975). The right to privacy. Philosophy and Public Affairs, 4(4), 295–314.

U.S. Department of Health. (1973). Records, computers and the rights of citizens. Washington, D.C.: U.S. Department of Health and Human Services.

United Nations. (1945, June 26). Charter of the United Nations. Retrieved from https://www.un.org/en/charter-united-nations/index.html

United Nations. (1948, December 10). Universal Declaration of Human Rights. Retrieved from https://www.un.org/en/universal-declaration-human-rights/index.html

Upward, A. and Jones, P. (2015). An ontology for strongly sustainable business models: Defining an enterprise framework compatible with natural and social science. Organization and Environment, 29(1), 97–123.

Véliz, C. (2021). Privacy and digital ethics after the pandemic. Nature Electronics 4, 10-11.

Wang, R. (2013, June 13). Beware trading privacy for convenience. Retrieved from Harvard Business Review: https://hbr.org/2013/06/beware-trading-privacy-for-con

Warren, S. and Brandeis, L. (1890). The right to privacy. Harvard Law Review, 4(5), 193–220.

Wells, P. (2013). Business models for sustainability. Cheltenham: Edward Edgar.

West, S. M. (2017). Data capitalism: Redefining the logics of surveillance and privacy. Business and Society, 58(1), 20–41.

Westerman, G. and Bonnet, D. (2015). Revamping your business through digital transformation. MIT Sloan Management Review, 3(56), 2–5.

Westin, A. F. (1967). Privacy and freedom. New York: Atheneum.

World Commission on Environmental Development. (1987). Our common future. Oxford, England: Oxford University Press.

World Health Organization. (2021). Ethics and governance of artificial intelligence for health: WHO guidance. Geneva: WHO.

World Economic Forum. (2021). The Global Risks Report 2021. Retrieved from http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

Zott, C., Amit, R. and Massa, L. (2011). The business model: Recent developments and future research. Journal of Management, 37(4), 1019–1042.

About the Authors

Fabien Rezac is a PhD Fellow at the Interdisciplinary Centre for Digital Business Development, Department Business Development and Technology, Aarhus University, Denmark, and a Recognised DPhil Student at the Saïd Business School, University of Oxford, UK. He holds an award-winning MSc degree in Economics and Business Administration, has consultancy experience from Deloitte, managerial experience from the public as well as non-profit sector, and conducted research for European Commission. In his research, he focuses on exploring the dynamics of management and business development in relation to technology and sustainability.