Contents lists available at ScienceDirect

Fundamental Research

journal homepage: http://www.keaipublishing.com/en/journals/fundamental-research/

Article

Managing privacy in the digital economy

Chong Wang[a], Nan Zhang[b,*], Cong Wang[a]

[a] Guanghua School of Management, Peking University, Beijing, China
[b] School of Management, Harbin Institute of Technology, Harbin, China

ARTICLE INFO

Article history:
Received 27 April 2021
Received in revised form 19 August 2021
Accepted 22 August 2021
Available online 3 September 2021

Keywords:
Digital Economy
Privacy
Privacy Concern
Privacy Calculus
Differential Privacy

ABSTRACT

In this era of the digital economy, proper management of digital privacy is critical for end-users, service providers, platform vendors, and the government. Addressing the increasing privacy concerns expressed by the public, research on digital privacy steadily grew over the recent decade, covering management, economics, and information science. Relevant regulation policies have also been adopted to control data privacy and the processing of personal data by digital service providers. As academic discussions accumulate, a convolution of conceptualizations of digital privacy emerges, which obstructs the interdisciplinary research progress. Based on a comprehensive review of related literature, this paper proposes an ontology of digital privacy and discusses emerging research themes. This paper emphasizes the interdisciplinary nature of privacy-related issues and provides the foundation for a merged view and practice-focused solutions.

1. Introduction

The collection and usage of digital data have become indispensable for the business process. Information technology (IT) development continues to push digitization forward. Online platforms, smart devices, and artificial intelligence (AI) applications have influenced many aspects of personal life, including commerce, social networking, transportation, and education. In the era of big data, the automatic collection of nano-level personal data empowers advancements in AI and data mining algorithms that generate unprecedented consumer insights and enables valuable personalized services. At the same time, the collection and usage of digital personal data and their negligent handling by online platforms endanger privacy. Privacy violation incidences are frequently reported and debated, causing significant privacy concerns and anxiety among consumers of digital services. Therefore, there is an urgent need for proper management systems and regulatory policies to govern privacy-related practices in the big data era.

Significant research efforts have been exerted towards understanding digital privacy from different perspectives. Discussions in the information systems literature conceptualize information privacy in the context of e-commerce transactions and online social networking; the antecedents and consequences of information privacy concerns are explored, thus shedding light on the management of customer privacy [1–4]. Economists have studied the economic trade-off between privacy and the use of online services [5–7]. In the field of technology, research efforts have focused on understanding the inference of personal information from shared data [8], to improve the security of information systems [9], and create algorithms that enable data transactions without undermining privacy [10].

Digital privacy is an interdisciplinary concept. On the one hand, advances in information technology prompt the collection and use of personal data while providing tools to protect and manage privacy. On the other hand, privacy protection extends to protecting both the personal space and psychological independence on the Internet beyond personal data. As digital and online social interactions continue to flourish and because of the increasingly ubiquitous merging and sharing of nano-level personal data, privacy issues need to be handled appropriately to protect users, while simultaneously empowering the development of the digital economy. However, current academic discussions about digital privacy adopt different theoretical lenses, conceptualizations, and methodologies. A systematic conceptual framework is thus needed to facilitate interdisciplinary research on digital privacy and form an overarching research agenda to empower digital privacy management. This paper develops an ontology of digital privacy combining behavioral, economic, and technical perspectives, based on a comprehensive yet concise review of extant research on digital privacy [4,5]. According to the available discussions and the role digital platforms play in managing privacy, a framework is proposed for managing digital privacy from the perspective of boundary resources theory [11]. Moreover, emerging issues for future privacy research are discussed.

[*] Corresponding author.
E-mail addresses: alexwang@gsm.pku.edu.cn (C. Wang), andyzhang@hit.edu.cn (N. Zhang), wangcong@gsm.pku.edu.cn (C. Wang).

https://doi.org/10.1016/j.fmre.2021.08.009

2. Digital privacy research

Digital privacy is a multifaceted concept. In social psychology, privacy is defined as the selective control of access to the self. From an economic perspective, privacy relates to the disutility from losing control of and the risk associated with releasing personal information. Enabled by AI and big data technologies, digitalization of personal life and smart applications extend the conceptualization of privacy to digital privacy. The following provides a review of the privacy research development from three perspectives—privacy as a fundamental psychological need, privacy as an economic trade-off, and privacy as a technical artifact.

2.1. Privacy as a fundamental psychological need

Privacy is, at its core, a psychological concept. Digital privacy represents an important line of privacy research in information systems (IS). The earliest conceptualization of information privacy in the IS literature was proposed by Smith et al. [3]. They pioneered a series of studies that developed the multidimensional information privacy concept of the concern for information privacy (CFIP). CFIP captures individuals' concerns about organizational information privacy practices. It includes four dimensions: collection (i.e., the degree to which a person is concerned that extensive personally identifiable data are being collected and stored in databases), unauthorized secondary use (i.e., the degree to which a person is concerned that information is being collected from individuals for one specific purpose, but is then also used for another, secondary purpose, without authorization from the individuals), improper access (i.e., the degree to which a person is concerned that data about them are readily available to people not properly authorized to view or work with these data), and errors (i.e., the degree to which a person is concerned that protective mechanisms against deliberate and accidental errors associated with the access of personal data are inadequate).

With the development of Internet applications, researchers expanded the concept of information privacy as the degree to which an Internet user is concerned about the practices related to the collection and use of personal information. Drawing on social contract theory, Malhotra et al. [2] developed the multidimensional information privacy concept Internet users' information privacy concerns (IUIPC), which has three dimensions: collection, control (i.e., the degree to which a person is concerned that she does not have adequate control over her personal information held by websites), and awareness (i.e., the degree to which a person is concerned about her awareness of information privacy practices by websites). By synthesizing prior research and integrating CFIP and IUIPC, Hong and Thong [1] proposed a new factor structure of information privacy: Internet privacy concerns (IPC). IPC includes two second-order factors (i.e., interaction management and information management) and six first-order factors (i.e., collection, secondary usage, errors, improper access, control, and awareness). Recognizing the proliferation of mobile technologies and smartphones, Xu et al. [12] drew on the communication privacy management theory [13] and developed a mobile users' information privacy concerns (MUIPC) scale that contextualizes information privacy concerns to mobile computing. MUIPC includes three dimensions: perceived surveillance, perceived intrusion, and secondary use of personal information. Similar to previous conceptualizations, MUIPC focuses on information transactions between users and service vendors.

Recent studies have focused on privacy issues associated with online social networking in response to the rapid diffusion of social media applications. Privacy has been considered as either an antecedent or a consequence of online social interactions. For example, Hu et al. [14] proposed that online social value combines utilitarian and hedonic benefit, information risks, and effort. Yu et al. [15] showed that personal affect influences self-disclosure in online social networks both directly and indirectly. Ozdemir et al. [16] found that trust, risk, benefits, and privacy concerns together explain a significant share of the variance in disclosure behaviors. These studies considered several peer-related privacy constructs. For example, Ozdemir et al. [16] found that peer-focused privacy experiences and privacy awareness are significant predictors of peer-related privacy concerns. In an experimental study, Choi et al. [17] found evidence that information dissemination and network commonality jointly influence individuals' perceived privacy invasion and perceived relationship bonding in case of exposure of embarrassing content. Liu et al. [18] focused on role conflict in online social networks and showed that role conflict influences both privacy risk (concerns) and perceived control.

Privacy needs exceed the protection of personal information as online social networks expand to more domains of private life. Lin and Armstrong [19] proposed that individual privacy management in social networking services needs to consider both information privacy and territory privacy. By revisiting the psychological foundation of privacy, Zhang et al. [4] proposed a new construct called peer privacy concern (PrPC) and defined it as the general feeling of being unable to maintain functional personal boundaries in online activities as a result of the behaviors of online peers. Rooted in the theory of personal boundaries and building on extant privacy research, PrPC consists of four dimensions: information privacy concern, virtual territory privacy concern, communication privacy concern, and psychological privacy concern. PrPC provides a comprehensive conceptual foundation for understanding the impact of new technologies, such as open platforms and AI, on digital privacy.

2.2. Privacy as economic trade-off

While being a psychological need, privacy has a real and significant economic impact. Economists have long been interested in understanding the economic value and consequences of the disclosure of personal information and the decision process for sharing personal data [5]. Studies in the areas have addressed the general value of privacy [20], the prevalence of asymmetric information and adverse selection [21], the transmission of private information through signaling activity [22], voluntary disclosures [23], the economic claim over personal data [24], the transfer of the rights to personal data [25], consumer identification [26], price discrimination [27], data intermediaries [28], the data market [6], and marketing techniques [29]. Despite the richness of extant research, there is no unified definition of privacy in economics. Instead, economists treat privacy as a context-dependent control of the boundary between the self and others. The economics of privacy, therefore, concerns the trade-offs associated with balancing public and private spheres between individuals and their environments [5].

The Internet has evolved from an architecture of decentralized and anonymous interactions [30] to an architecture where data capturing various types of behaviors are uniquely [31] and personally [32] identifiable. Leveraging the value of such a vast amount of personal information, new services, new companies, and new markets have emerged [33]. Despite the benefits of data, public concerns over personal privacy violations have also increased, as shared personal information becomes a non-rivalry and non-excludability public good. The value of protecting and disclosing personal information is context-dependent and contingent on essentially uncertain combinations of states of the world [5]. The disclosure of personal data likely generates trade-offs with economic dimensions. Individuals can directly benefit from sharing their data to obtain personalized services or discounts. However, the costs of doing so are often uncertain and generally incur at a distant point in time [5].

The decision of personal information disclosure is a function of the calculation of potential benefits and costs. To this end, privacy calculus theory—rooted in libertarian political sciences and economics [34,35]—focuses on the economic attributes of privacy rather than on its absolute value [36]. The central tenet of the privacy calculus perspective is that privacy transactions are evaluated in economic terms [37]. Theories like communication privacy management (CPM, [13]) were developed based on this logic. However, in most cases, it is difficult for consumers to make informed decisions about their privacy because of the existing information asymmetry. The resulting discrepancy between attitude and behavior toward personal information disclosure is known as the *privacy paradox*.

Researchers proposed that the privacy paradox is driven by bounded rationality, e.g., dual-process thinking [38]. Phelan et al. [39] suggested that both intuitive privacy concern and considered privacy concern influence the evaluation of personal information disclosure. According to their study, a privacy paradox emerges when a considered assessment overrides an intuitive assessment without eliminating it. Similarly, Liu et al. [18] identified a dual process in people's decision making on information disclosure. Specially, they showed that emotion can moderate the evaluation of perceived privacy risk. Based on the elaboration likelihood model (ELM), Wang et al. [40] found that self-disclosure intention develops along a dual route including a central route and a peripheral route. If the central route predominates, people's privacy behavior will be more rational, while if the peripheral route predominates people's privacy behavior will be more emotional. In summary, the main idea of this dual process is that environmental constraints may affect rational thinking, while unconscious bias may affect irrational thinking. Both will lead to inconsistency between privacy attitude and behavior [41]. Nevertheless, in general, most previous studies in this area agreed that information disclosure is not always harmful to the individual and may improve the welfare of all parties involved [7,42].

2.3. Privacy as a technical artifact

Digital privacy is also a technical artifact. Privacy concerns are not only caused directly by technological development, and research efforts have also been dedicated to addressing data privacy issues and enabling digital privacy management. Various privacy models have been proposed, including k-anonymity, l-diversity, t-closeness, and differential privacy models.

A popular traditional privacy model is the k-anonymity model, which requires that an individual is not identifiable from a group of size smaller than k [43,44]. The k-anonymity model fails in cases with predominant sensitive attribute values. To overcome this vulnerability, other variant privacy models have been proposed with assumptions on sensitive attribute value distributions, including the l-diversity model [45] and the t-closeness model [46]. Specifically, l-diversity requires the sensitive attributes to take at least l values, while t-closeness adds assumptions on the closeness between the distribution of sensitive attributes and the overall attribute distribution. Although widely adopted, these models are vulnerable to uncontrolled background information [47].

Differential privacy (DP) is another privacy model with strong standards [48]. The aim of DP is to mask computation divergence on neighboring datasets with one different data entry at most, thus not revealing too much information about any individual record in the dataset. Concretely, given two neighboring datasets D and D' with at most one different data element, a randomized mechanism M can yield (ϵ, δ)-differential privacy for every set of outputs S, if M satisfies:

$$\Pr\left[M(D) \in S\right] \leq \exp(\epsilon) \cdot \Pr\left[M\left(D'\right) \in S\right] + \delta$$

where ϵ is the privacy budget controlling the privacy guarantee level, with smaller ϵ representing stronger privacy. δ is an accuracy parameter, i.e., if $\delta = 0$, M can yield ϵ-DP by its strictest definition, while $\delta > 0$ can yield (ϵ, δ)-DP, which provides certain freedom to violate pure DP for specific low-probability events. Unlike previous privacy models, very loose assumptions are imposed on the background information of the adversary in DP. Therefore, DP can handle most privacy attacks with a provable statistical guarantee. To achieve DP, noise is added to the output of the algorithm. Two commonly adopted mechanisms are Laplacian and Gaussian mechanisms [49]. With the introduction of moments accountant and the differentially private stochastic gradient descendent (SGD) algorithm [10], the implementation of DP has become more practical, and various deep-learning-based DP preservation algorithms have been proposed [9,50,51]. DP has been widely applied to solve privacy concerns in various fields, such as social network analytics [52], recommender systems [53,54], and spatial crowdsourcing [55,56].

With the prevalence of multi-party cooperations, how privacy can be ensured throughout collaborations has become a prominent problem. A recent stream of literature attempted to solve this problem through federated learning (FL) [57,58]. The idea of FL is to develop machine learning models with distributed datasets on multiple devices (while preventing data leakage), through which privacy can be enforced. FL can be categorized into horizontal FL, vertical FL, and federated transfer learning (FTL) [59]. In horizontal FL, the distributed datasets share the same feature space, and thus, machine learning models can be computed locally and send the masked results to a centralized server, where model aggregation is performed and the results are sent back for local update [60,61]. In vertical FL, decentralized datasets share similar sample identities but differ in feature space. In such cases, encrypted entities of different parties are aligned first, and local model training is then performed through the exchange of encrypted intermediate results, where a collaborator is used to generate encryption pairs with public keys [59]. In FTL, isolated datasets have small overlaps, and hence, transfer learning is needed to extend the knowledge to a different domain. As FL lacks a theoretical guarantee on its own, its consolidation with theoretically guaranteed privacy-preserving mechanisms is an emerging research topic. Recent research efforts combined DP and FL to achieve multi-party privacy preservation [62,63].

While privacy and information security have distinct concerns, they can overlap depending on research targets. Information security refers to processes designed to protect data assets. Poor information security can lead to what Solove [64] referred to as insecurity or carelessness in protecting personal information from leaks and improper access. However, a security system may also endanger privacy. For example, to protect users from junk mail, incoming emails are scanned by the server first, which may violate the privacy of both the sender and the receiver.

Table 1 summarizes exemplary publications on digital privacy in different domains reviewed in the text above. While this list is not intended to be exhaustive, it provides an overview of important streams and shows the diversity in digital privacy research.

2.4. Digital privacy – towards an ontology

Based on the review of previous research, an ontology of digital privacy is proposed (Fig. 1), considering the psychological, economical, and technical aspects of privacy issues in digital economy. Digital privacy is defined as the selective psychological and technical control of access to the digital self in the form of online profiles, personal data, and digital assets. The proposed ontology reflects the cumulative body of knowledge on privacy issues in the digital world and exhibits the logical relations between concepts.

Five core concepts emerged from extant academic discussions about digital privacy: digital privacy, personal boundary management, personal data management, privacy concern, and privacy coping.

At the center of digital privacy is the need for an individual to differentiate oneself from the social environment for establishing and maintaining an intact self-concept and individuality—the personal boundary management process [65]. In other words, personal boundary management defines the self as a unique individual and privacy claim [4]. Digital technologies create an individual's digital representation in the virtual space. With the development of digital economy, this digital representation evolved from being a collection of personal data (personal data management needs) to being a integral part of the self-concept—the virtual self [66]. In the digital economy, individuals virtually interact with a variety of peers in the contexts of online communities, e-commerce, online services, and online social networks with their digital identities. Such online social intereactions blur the natural boundaries that help individuals to control the adopted identity and maintain self-concepts [67]. For example, the proliferation of instant communication tools adopted in working situations leads to the increasing overlap of

Table 1
Representative studies on digital privacy.

Privacy as a Fundamental Psychological Need	
Development of measurements of privacy concerns	CFIP [3], IUIPC [2], MUIPC [12], IPC [1], and PrPC [4]
Antecedents and consequences of privacy concerns	Privacy risk [14–18] and peer influence [19]
Privacy as Economic Trade-off	
Economic value of disclosing personal information	General value of privacy [20], transmission of private information through signaling activity [22], economic claim over personal data [24], transfer of the rights to personal data [25], price discrimination [27], and the data market [6]
Personal information disclosure decision	Communication privacy management [13] and the dual-process model [38]
Privacy as a Technical Artifact	
Anonymization-based methods	k-anonymity method [43,44], l-diversity method [45], and t-closeness method [46]
Differential privacy (DP) model	Noise-adding methods [48], differentially private SGD algorithm [10], and deep-learning-based differential privacy preservation algorithm [9,50,51]
Federated learning (FL) methods	Horizontal federated learning [60,61], vertical federated learning [59], and federated transfer learning [59]
Combination of DP and FL	Multi-party privacy preservation [62,63]

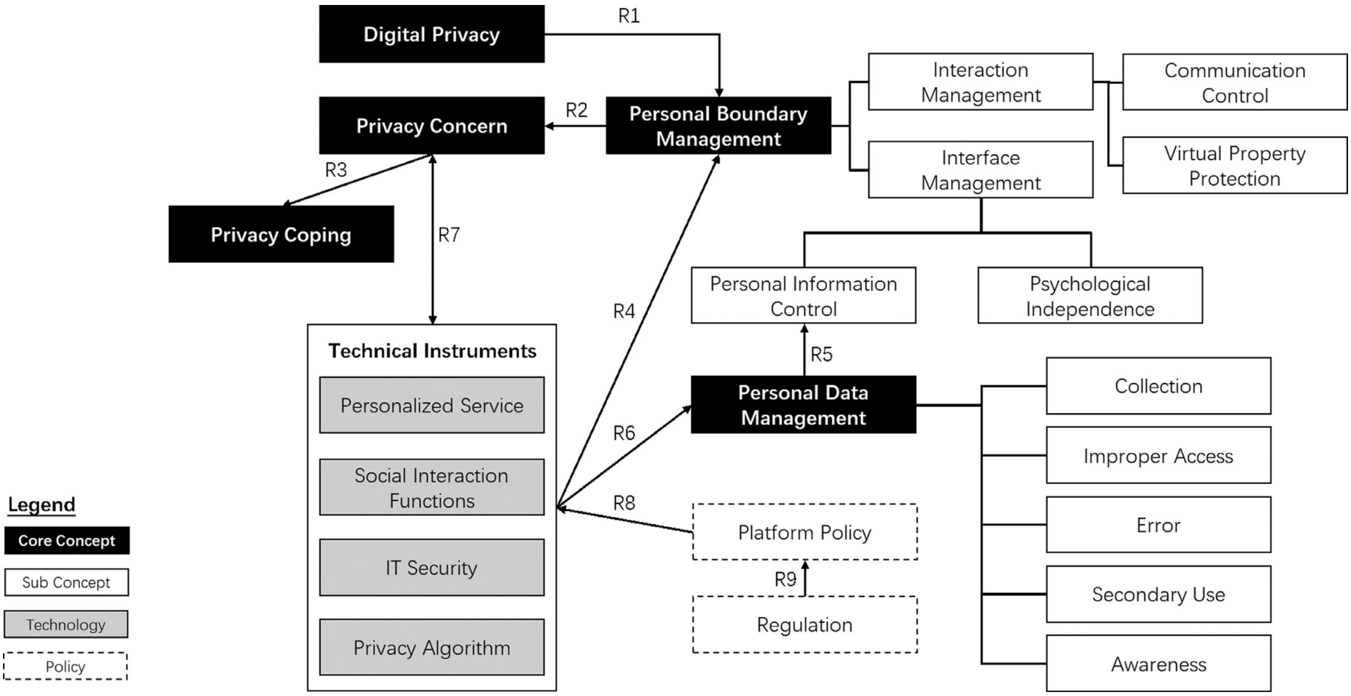

Fig. 1. Digital privacy ontology.

work and family subsystems, resulting in greater work-family conflicts [68,69]. Effective personal boundary management enables individuals to demarcate boundaries in their work and nonwork roles [70].

Personal boundary management governs six sub-concepts in two layers (e.g., [4]), and personal data management governs five sub-concepts (e.g., [1,3]). While the concept of personal data management concerns primarily the interaction between platform owners (i.e., service vendors) and users, digital privacy directly relates to personal boundary management in all types of social interactions, covering personal data management as a core subdomain. Lack of control in personal boundary management results in privacy concerns, which induce privacy coping effort. Platforms empower/endanger personal boundary management by designing and implementing technical instruments that form the environment for privacy coping behavior. Privacy regulation governs the setting of platform policy that informs the design of technical instruments. Accordingly, nine relations are extracted and the premises governing these relations are discussed (Table 2). Example (review) papers are included for extended reading.

The following insights presented in the ontology are highlighted (relations and fundamental premises). First, digital privacy is an extension to the psychological privacy need of the digital/online social environment. While the current focus and a critical component of digital privacy management is the management of personal data (data-related technology and policies), individuals' privacy concerns extend to the preservation of personal spaces, and thus, personal boundary management. Second, perceived control over the personal boundary and, more specifically, personal data is determined by the design and implementation of technical instruments not necessarily intended for privacy management. For example, while commenting and tagging functions in a social networking application intend to facilitate social interactions, these may undermine the perceived control over the interpersonal boundary and raise privacy concerns. Third, to cope with privacy concerns, different types of coping behaviors (e.g., avoidance, voicing, or acceptance) can be implemented depending on the perceived control over the situation and partly determined by the affordance of technical instruments. Fourth, privacy trade-offs mix tangible with intangible benefits. The economics of privacy concerns the trade-offs associated with the balancing of public and private spheres beyond the traditional focus on the economic consequences of disclosing personal data. Fifth, new big data technologies (including DP and FL), are important additions to the technical instruments deployable by platforms and may help in quantifying privacy protection and the introduction of market mechanisms for privacy management. Sixth, platforms' privacy policies are implemented through (and thus reflected in) platform system design. The design and impact of privacy regulations depend on technical instruments and market mechanisms for personal data transactions.

Table 2
Relationships between core concepts.

Relations	Foundational Premises (FPs)	Papers for Extended Reading
R1: Digital privacy is a personal boundary management process.	FP1: In the digital society, personal boundary management extends to virtual spaces to enable the development of the self-concept.	[4,71,72]
R2: Lack of control in personal boundary management results in privacy concerns.	FP2: Privacy concern results from the perceived (lack of) control over the personal boundary management process.	[2,18,73]
R3: Privacy concern leads to privacy coping.	FP3: Privacy concern leads to stress that induces different coping efforts (behaviors) depending on the social/technical environment. FP4: Coping behavior is constrained by the technical instruments the platform provides.	[74,75]
R4: Platforms' technical instruments enable (or endanger) personal boundary management.	FP5: Platforms design and implement functions to empower digital personal boundary management. FP6: Platform functions such as online profile management, online chat, and comments influence perceived and actual capability to control personal boundaries.	[76,77]
R5: Platforms' personal data management practices enable users' personal information control.	FP7: Platforms' personal data management practices, such as collection, secondary usage, access control, and policy transparency, influence the perceived control over personal information.	[1,2,12]
R6: Platforms' technical instruments constitute platforms' personal data management practice.	FP8: Platforms implement personal data management through the design of platform functions, including personalized services, social interaction functions, security, and privacy algorithms.	[10,43,48,49]
R7: [Privacy Calculus] Individuals balance between the benefit obtained from using technical instruments and digital privacy.	FP9: Utility related to privacy mixes tangible (e.g., risk associated with sharing personal data) and intangible returns (e.g., psychological discomfort associated with loss of control). FP10: The trade-off structure between service value and privacy is determined by the platform's technical environment, including the provision of personalized services, the level of security, and the application of privacy algorithms. FP11: Individuals are heterogenous in their preference for privacy and digital services. Their preferences are revealed through their actions and choices.	[36,37,78]
R8: Platform policies inform the design of technical instruments.	FP12: Platforms should have explicit policies regarding digital privacy protection to inform both users and the implementation of technical functions.	[1,79]
R9: Regulation policies govern platform policies.	FP13: Regulation policies should cover privacy protection comprehensively. FP14: Platforms adjust policy settings according to both regulations and business interests.	[80,81]

3. Managing privacy on digital platforms

The digital privacy ontology discussed here provides an overarching framework for understanding issues related to privacy in the digital economy. It decomposes privacy into sub-concepts that drive individuals' online behavior and, more importantly, clarifies and highlights the roles of technological artifacts, platform governance, and regulation policies in the process of digital privacy management. Digital privacy discussions center on the creation, evolution, and management of online platforms. These platforms (e.g., e-commerce, social networking services, and online financial services) should address digital personal data protection issues, and they should also orchestrate the technical environment for online participation so that privacy concerns are minimized. Recognizing the role of digital platforms and informed by this ontology, the boundary resource perspective is proposed as a valuable theoretical lens for unifying multi-disciplinary discussions and understanding privacy management practice in the digital economy that center around online platforms fueled by personal data.

3.1. Digital platform governance – the boundary resource perspective

Addressing privacy issues in the digital economy should focus on managing and regulating platforms that serve as interfaces for personal data and digital interaction. Tiwana et al. [11] defined a digital platform as "the extensible codebase of a software-based system that provides core functionality shared by the modules that interoperate with it and the interfaces through which they interoperate." Digital platforms emerged with the development of the digital revolution and have penetrated many industries, including e-commerce, social networking services, transportation, financial services, healthcare, education, and industrial production management. The platform approach to product development derives from the general idea that it is economical to reuse core parts of existing products and technologies to create new products that serve broader customers [82–84]. The core product serves the needs of the core audience (e.g., the operating system and default apps), while the needs of the broader audience are served through a complementary set of components (e.g., third-party apps) [85,86]. In a platform economy, platform owners orchestrate interactions between service/product providers (developers) and customers by providing boundary resources.

Boundary resources refer to "the software tools and regulations that serve as the interface for the arm's length relationship between the platform owner and the application developer" [87]. Boundary resources play a critical role in resolving the paradoxical tension between a platform owner's need to secure control over both infrastructure and service system and the necessity to allow free, empowered participation of independent firms in the platform-based ecosystem. The role of application developers in the platform ecosystem has been studied [88,89]. Eaton et al. [90] showed that developers' accommodations and rejections can tune a platform owner's boundary resource provision decisions. Moreover, research has also shown that resource provision has important implications on the institutional logic in a platform-based ecosystem [91,92].

While alien to the current research on digital privacy, boundary resource theory provides a useful framework that helps to unify interdisciplinary discussions on privacy. Digital platforms serve as an interface between platform stakeholders and manage the complex relationships between them, including privacy issues in service transactions [87,90,93,94]. Fig. 2 illustrates the framework of interactions between stakeholders of a platform ecosystem from a boundary resources management perspective.

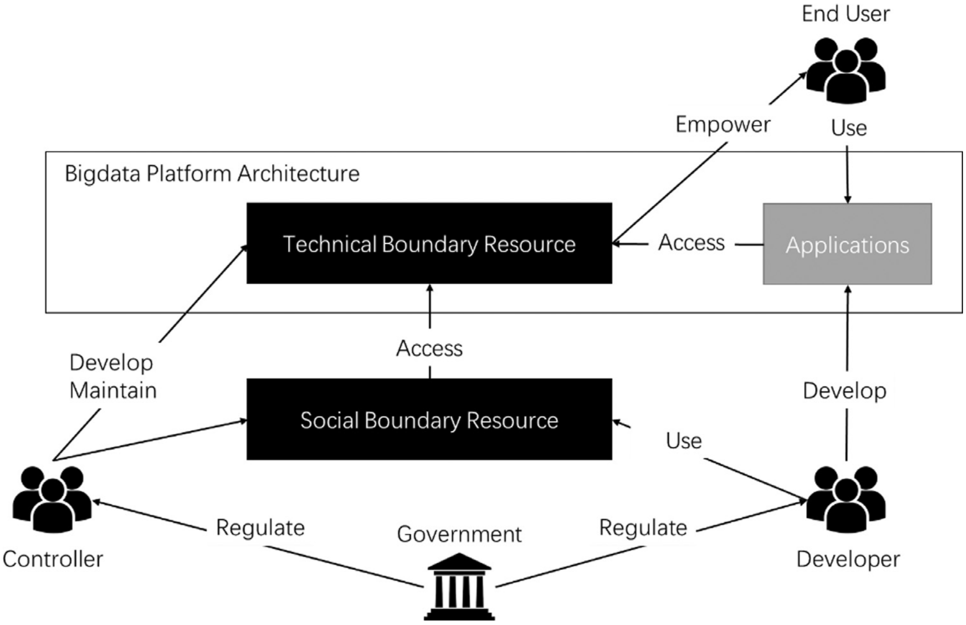

Fig. 2. Boundary resource perspective.

3.2. The management of digital privacy as boundary resources

Regarding digital privacy, stakeholders of a platform play distinct roles and have different demands. End-users choose and use applications according to their value perceptions. They may experience, or be aware of, privacy violations and either consciously or subconsciously make a trade-off between usage and privacy. They desire guarantees of privacy protections and actively seek help in managing privacy. Developers provide services/products to end-users and strive for financial returns. They may customize their service/product taking advantage of access to personal information and may seek opportunities to exploit access to personal information. Their interactions with end-users are moderated by platform architecture and governed by policies and mechanisms set by platform owners. Platform owners take care of both developers and end-users to generate positive network effects. In doing so, they need to balance private data collection (e.g., usage data) and privacy protection. They need to design data transfer mechanisms, maintain system security, set and enforce privacy protection rules, and provide tools that empower end-users to manage their privacy. Their practice is governed by regulatory constraints the aim of which is to protect end-users and improve social welfare.

The provision of boundary resources implements the management of digital privacy. On the technical side, boundary resources, such as platform APIs and SDKs, act as necessary governance devices. They provide technical feasibility for app development and enable app integration with platform architecture. The transfer of personal data and developers' interactions with end-users is implemented by designing technical boundary resources. Furthermore, platforms may provide end-users with tools to track and manage their personal information and control their social interactions on the platforms, thus empowering privacy control at the user side and alleviating privacy concerns. For the government, technical boundary resource provision can enable process-driven privacy regulation and the real-time monitoring of privacy protection. On the social side, platforms orchestrate and control market interactions between developers and end-users through mechanism design and policy setting. On the one hand, platform policies govern developers' dealing with end-user privacy. On the other hand, the market mechanism enables the transfer of and proper compensation for personal data, thus shaping the business models of developers. The implementation of boundary resources determines interaction feasibilities between stakeholders of big data platforms. As a result, boundary resources serve as focal constructs that unite discussions about privacy management in big data platforms.

3.3. Extending digital privacy research

Combining the ontology of digital privacy and boundary resource perspectives enables the discovery of promising and important research questions about digital privacy. In the following, a number of areas are proposed that deserve future research effort. While it is important to continue expanding research in each of the three streams of literature reviewed in this paper, it is also critical to foster interdisciplinary perspectives for understanding the privacy implications of cutting-edge information technology development and changing the market environment. Table 3 lists exemplary questions in each question area.

3.3.1. Question area I: behavioral impact of big data privacy

Discussions about information privacy concerns in the context of e-commerce have been extensive. However, the proliferation of digital services fundamentally changed the implications of big data technologies on individuals' psychological wellbeing. Discussions about the behavioral impact of digital privacy need to be extended to embrace changes in the social information environment. Research attention should move beyond the constrained focus on personal information disclosure and also discuss the psychological implications and coping behaviors of privacy issues resulting from peer-oriented online interactions. Research should also start to discuss the behavioral impact of technical artifacts, such as interaction process design, third-party personalization services, privacy management tools, and smart tracking devices, on privacy concerns to generate concrete design principles that address privacy needs.

3.3.2. Question area II: economic consequences of privacy management and regulations

The protection of digital privacy is fundamental to the development of the digital economy and has received significant attention from regulators. Despite these efforts, the economic impact of privacy protection remains ambiguous, which hinders policy development and innovative business model development. Research should start to address the welfare implications of privacy, especially from an empirical perspective. Moreover, privacy concerns are likely to influence how people engage in

Table 3
Extending digital privacy research.

Question Area	Perspective	Example Questions
Behavioral Impact of Big Data Privacy	Behavioral	How does the (network) structure of online social interactions among peers affect privacy concerns? How are users coping with privacy concerns induced by peer interactions? How does the technical environment influence their choice of coping strategy?
	Behavioral, Technical	What are implications of advanced interactive artificial intelligence (AI) agents on privacy? How to design an AI agent to handle privacy concerns effectively? How to design platform interactions to empower privacy management?
	Behavior Economic	Do users make the same trade-off for different dimensions of privacy needs? What is the value function for privacy?
Economic Consequences of Privacy Management and Regulations	Economic	How to quantify the economic trade-off between privacy and service value? What are welfare and economic consequences of privacy regulation? How to design privacy regulations to improve social welfare? How to design a privacy-oriented mechanism to enable personal information disclosure and data sharing?
Technical Solutions for Managing Big Data Privacy	Technical	Apart from membership privacy governed by the differential privacy model, are there any other types of data privacy issues? If so, how can privacy concerns be alleviated simultaneously in the privacy-preserving algorithm design? How can process-driven privacy regulation be implemented?
	Technical, Economic	How can the value of private data be measured from the perspective of a privacy algorithm? When coordinating multiple parties, how should the privacy budget be allocated to each party, and what is the impact of different privacy budget allocations? How to design incentive-compatible incentive mechanisms for the federated-learning framework so that each participant is willing to contribute to the joint learning objective?

economic transactions with their peers, resulting in unique equilibrium behavior in business social networks. Further, the quick development of privacy algorithms and blockchain technologies enables new privacy management instruments that empower privacy management beyond awareness. Future research could propose innovative privacy-oriented economic mechanisms, such as incentive-compatible mechanism design when trading off privacy with service value.

3.3.3. Question area III: technical solutions for managing big data privacy

Privacy is a trade-off in nature, and the structure of this trade-off depends on the technology solutions for personal data management. First, privacy protection and regulation rules call for research on new big data privacy algorithms that generate a more comprehensive understanding of the nature of digital privacy and a quantitative measure of privacy protection effectiveness. The development of such algorithms enables more accurate privacy management but also sheds light on evaluating data value in exchange. Second, data merging and data transactions are essential to the development of digital business models. The proliferation of data transactions essentially increases the complexity of the protection of information privacy. Technical solutions such as federated learning and blockchain systems are needed to nurture privacy-friendly data exchange markets. Third, the technical design of platform functions and API needs to fully consider their privacy implications from a data protection perspective as well as their impact on the psychological aspects of privacy.

4. Conclusion remarks

The development of data exchange, AI-based personal assistance, advanced Internet of Things (IoT) tracking capabilities, digital education, and healthcare calls for more effective privacy management and regulations to help individuals navigate the digital economy. Big data technologies serve as double-edged swords in the context of digital privacy. On the one hand, the development poses severe threats to privacy-concerning personal information disclosure, general psychological independence, and wellbeing. On the other hand, advancements in big data technologies provide new instruments for monitoring and managing digital privacy.

This paper attempts to untangle the convoluted discussions about digital privacy to foster interdisciplinary research progress. Based on a comprehensive review of the literature in different domains, an ontology of digital privacy is proposed and emerging research areas are discussed. The interdisciplinary nature of privacy-related issues is emphasized and the boundary resource perspective is suggested as a valuable theoretical lens to integrate the developments in digital privacy research. This paper adds clarity to digital privacy and promotes a merged view and practice-focused solutions. The following final remarks are presented to conclude the paper: First, while it is critical to continue to enrich discussions about data privacy, especially from a technical perspective, investigations of big data privacy should not be limited to protecting personal data. Privacy research should embrace the context changes in social interactions induced by IT development, including AI, smart mobile devices, and online platforms for data exchanges; the broader implications of digital technology on protecting personal spaces should be discussed. Second, the management and regulation of privacy could focus on designing and implementing platform boundary resources that include both the technical capability and system interaction design governed by platform policies. In addition to enforcing outcome-driven regulations and practice standardization, process-driven and penetrative regulatory practices and real-time privacy protection monitoring could be implemented, taking advantage of new technologies such as blockchain and privacy algorithms. Third, research should strive for a more comprehensive and scientific understanding of the long-term behavioral and economic consequences of privacy concerns. More research is needed to evaluate the effectiveness of privacy management practices and regulation policies.

Declaration of Competing Interest

The authors declare that they have no conflict of interest in this work.

Acknowledgments

Chong (Alex) Wang acknowledges support from National Natural Science Foundation of China (Grant No. 71501168). Nan (Andy) Zhang acknowledges support from the National Natural Science Foundation of China (Grant No. 92046007). Cong Wang acknowledges support from the National Natural Science Foundation of China (Grant No. 92046021).

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.fmre.2021.08.009.

References

[1] W. Hong, J.Y.L. Thong, Internet privacy concerns: an integrated conceptualization and four empirical studies, MIS Q. 37 (1) (2013) 275–298.

[2] N.K. Malhotra, S.S. Kim, J. Agarwal, Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model, Inf. Syst. Res. 15 ((4) (2004) 336–355.
[3] H.J. Smith, S.J. Milberg, S.J. Burke, Information privacy: measuring individuals' concerns about organizational practices, MIS Q. 20 (2) (1996) 167–196.
[4] N. Zhang, C. Wang, E. Karahanna, et al., Peer privacy concerns: conceptualization and measurement, MIS Q. (2021) forthcoming.
[5] A. Acquisti, C. Taylor, L. Wagman, The economics of privacy, J. Econ. Lit. 54 (2) (2016) 442–492.
[6] D. Bergemann, A. Bonatti, Markets for information: an introduction, Annu. Rev. Econ. 11 (2019) 85–107.
[7] J.H. Kim, L. Wagman, Screening incentives and privacy protection in financial markets: a theoretical and empirical analysis, Rand J. Econ. 46 (1) (2015) 1–22.
[8] D. Garcia, Leaking privacy and shadow profiles in online social networks, Sci. Adv. 3 (8) (2017) e1701172.
[9] J. Wang, W. Bao, L. Sun, et al., Private model compression via knowledge distillation, in: Proceedings of the AAAI Conference on Artificial Intelligence, 2019, pp. 1190–1197.
[10] M. Abadi, A. Chu, I. Goodfellow, et al., Deep learning with differential privacy, in: Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, 2016, pp. 308–318.
[11] A. Tiwana, B. Konsynski, A.A. Bush, Platform evolution: coevolution of platform architecture, governance, and environmental dynamics, Inf. Syst. Res. 21 (4) (2010) 675–687.
[12] H. Xu, S. Gupta, M.B. Rosson, et al., Measuring mobile users' concerns for information privacy, Proceeding of 33rd International Conference on Information Systems, Orlando, 2012.
[13] S.S. Petronio, Boundaries of Privacy: Dialectics of Disclosure (xix, pp. 268), State University of New York Press, Albany, NY, 2002.
[14] T. Hu, W.J. Kettinger, R.S. Poston, The effect of online social value on satisfaction and continued use of social media, Eur. J. Inform. Syst. 24 (4) (2015) 391–410.
[15] J. Yu, P.J.H. Hu, T.H. Cheng, Role of affect in self-disclosure on social network websites: a test of two competing models, J. Manag. Inform. Syst. 32 (2) (2015) 239–277.
[16] Z.D. Ozdemir, J. Smith, J.H. Benamati, Antecedents and outcomes of information privacy concerns in a peer context: an exploratory study, Eur. J. Inform. Syst. 26 (6) (2017) 642–660.
[17] B.C. Choi, Z. Jiang, B. Xiao, et al., Embarrassing exposures in online social networks: an integrated perspective of privacy invasion and relationship bonding, Inf. Syst. Res. 26 (4) (2015) 675–694.
[18] Z. Liu, X. Wang, Q. Min, et al., The effect of role conflict on self-disclosure in social network sites: an integrated perspective of boundary regulation and dual process model, Inf. Syst. J. 29 (2) (2018) 279–316.
[19] S. Lin, D. Armstrong, D. Beyond, Information: the role of territory in privacy management behavior on social networking sites, J. Assoc. Inf. Syst. 20 (4) (2019) 434–475.
[20] R.A. Posner, The right of privacy, GA. Law Rev. 12 (3) (1978) 393–422.
[21] G.A. Akerlof, The market for "lemons": quality uncertainty and the market mechanism, Q. J. Econ. 84 (3) (1970) 488–500.
[22] M. Spence, Job market signaling, Q. J. Econ. 87 (3) (1973) 355–374.
[23] S.J. Grossman, An introduction to the theory of rational expectations under asymmetric information, Rev. Econ. Stud. 48 (4) (1981) 541–559.
[24] E.M. Noam, Privacy and self-regulation: markets for electronic privacy, Privacy and Self- Regulation in the Information Age, US Department of Commerce, National Telecommunications and Information Administration, Washington, DC, 1997.
[25] K. Laudon, Extensions to the Theory of Markets And Privacy: Mechanics of Pricing Information, New York University Stern School of Business Working Paper, 1997 IS-97-4.
[26] D. Fudenberg, J. Tirole, Upgrades, tradeins, and buybacks, Rand J. Econ. 29 (2) (1998) 235–258.
[27] Y. Chen, Paying customers to switch, J. Econ. Manag. Strategy 6 (4) (1997) 877–897.
[28] A. Hagiu, B. Jullien, Why do intermediaries divert search? Rand J. Econ. 42 (2) (2011) 337–362.
[29] O. Shy, R. Stenbacka, Customer privacy and competition, J. Econ. Manag. Strategy 25 (3) (2016) 539–562.
[30] T. Berners-Lee, Weaving the Web: The Original Design and Ultimate Destiny of the World Wide Web, HarperCollins Publishers, New York, 2000.
[31] R. Bendrath, M. Mueller, in: The End of the Net as we Know It? Deep Packet Inspection and Internet Governance, 13, New Media Soc, 2011, pp. 1142–1160.
[32] Y. Xie, Y. Fang, M. Abadi, De-anonymizing the Internet using unreliable IDs, Comput. Commun. Rev. 39 (2009) 75–86.
[33] E. Schenk, C. Guittard, Toward a characterization of crowdsourcing practices, J. Innov. Econ. Manag. 1 (2011) 93–107.
[34] C. Bennett, Privacy in the Political System: Perspectives from Political Science And Economics, Ethical, Legal and Social Issues (ELSI) Component of the Human Genome Project, US Department of Energy, 2001.
[35] M.J. Culnan, P.K. Armstrong, Information privacy concerns, procedural fairness and impersonal trust: an empirical investigation, Organ. Sci. 10 (1) (1999) 104–115.
[36] D.I. Tamir, J.P. Mitchell, Disclosing information about the self is intrinsically rewarding, Proc. Natl. Acad. Sci. 109 (21) (2012) 8038–8043.
[37] B.C. Choi, Y. Wu, J. Yu, et al., Love at first sight: the interplay between privacy dispositions and privacy calculus in online social connectivity management, J. Assoc. Inf. Syst. 19 (3) (2018) 4.
[38] Z. Aivazpour, R. Valecha, R.H. Rao, Unpacking privacy paradox: a dual process theory approach, in: Proceedings of the Twenty-third Americas Conference on Information Systems, Boston, 2017.
[39] C. Phelan, C. Lampe, P. Resnick, It's creepy, but it doesn't bother me, in: Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 2016, pp. 5240–5251.
[40] L. Wang, H.H. Hu, J. Yan, et al., Privacy calculus or heuristic cues? the dual process of privacy decision making on Chinese social media, J. Enterp. Inf. Manag. 33 (2) (2020) 353–380.
[41] G. Gigerenzer, R. Selten, Bounded Rationality: The Adaptive Toolbox, MIT Press, 2002.
[42] B.C. Kim, J.P. Choi, Customer information sharing: strategic incentives and new implications, J. Econ. Manag. Strategy 19 (2) (2010) 403–433.
[43] P. Samarati, L. Sweeney, L. Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression, In Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, CA (1998).
[44] L. Sweeney, K-anonymity: a model for protecting privacy, Int. J. Uncertain. Fuzziness Knowl.-Based Syst. 10 (5) (2002) 557–570.
[45] A. Machanavajjhala, D. Kifer, J. Gehrke, et al., L-diversity: privacy beyond k-anonymity, ACM Trans. Knowl. Discov. Data 1 (1) (2007) 3-es.
[46] N. Li, T. Li, S. Venkatasubramanian, T-closeness: privacy beyond k-anonymity and l-diversity, in: Proceeding of 2007 IEEE 23rd International Conference on Data Engineering, 2007, pp. 106–115.
[47] R.C.W. Wong, A.W.C. Fu, K. Wang, et al., Minimality attack in privacy preserving data publishing, in: Proceedings of the 33rd International Conference on Very Large Data Bases, 2007, pp. 543–554.
[48] C. Dwork, F. McSherry, K. Nissim, et al., Calibrating noise to sensitivity in private data analysis, in: Theory Of Cryptography Conference, Springer, Berlin, Heidelberg, 2006, pp. 265–284.
[49] C. Dwork, A. Roth, The algorithmic foundations of differential privacy, Found. Trends Theor. Comput. Sci. 9 (3-4) (2014) 211–407.
[50] N. Papernot, S. Song, I. Mironov, et al., Scalable Private Learning with Pate, International Conference on Learning Representations, 2018.
[51] B. Wang, N. Hegde, Privacy-preserving q-learning with functional noise in continuous state spaces, (2019) arXiv:1901.10634.
[52] H. Y. Tran, J. Hu, Privacy-preserving big data analytics a comprehensive survey, J. Parallel Distrib. Comput. 134 (2019) 207–218.
[53] X. Liu, A. Liu, X. Zhang, Z. Li, et al., When differential privacy meets randomized perturbation: a hybrid approach for privacy-preserving recommender system, in: Proceeding of International Conference on Database Systems for Advanced Applications, Springer, 2017, pp. 576–591.
[54] F. McSherry, I. Mironov, Differentially private recommender systems: building privacy into the netflix prize contenders, in: Proceedings of the 15th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, 2009, pp. 627–636.
[55] J. Wei, Y. Lin, X. Yao, et al., Differential privacy-based location protection in spatial crowdsourcing, IEEE Trans. Serv. Comput. (2019) Early Access.
[56] Y. Xiao, J. Gardner, L. Xiong, Dpcube: releasing differentially private data cubes for health information, in: Proceeding of 2012 IEEE 28th International Conference on Data Engineering, 2012, pp. 1305–1308.
[57] J. Konečný, H. B. McMahan, D. Ramage, et al., Federated optimization: distributed machine learning for on-device intelligence, (2016) arXiv:1610.02527.
[58] J. Konečný, H. B. McMahan, F. X. Yu, et al., Federated learning: strategies for improving communication efficiency, (2016) arXiv:1610.05492.
[59] Q. Yang, Y. Liu, T. Chen, et al., Federated machine learning: concept and applications, ACM Trans. Intell. Syst. Technol. 10 (2) (2019) 1–19.
[60] Y. Aono, T. Hayashi, L. Wang, et al., Privacy-preserving deep learning via additively homomorphic encryption, IEEE Trans. Inf. Forensic Secur. 13 (5) (2017) 1333–1345.
[61] K. Bonawitz, V. Ivanov, B. Kreuter, et al., "Practical secure aggregation for privacy-preserving machine learning", in: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, 2017, pp. 1175–1191.
[62] R. C. Geyer, T. Klein, M. Nabi, Differentially private federated learning: a client level perspective, (2017) arXiv:1712.07557.
[63] A. Triastcyn, B. Faltings, Federated learning with Bayesian differential privacy, in: Proceeding of 2019 IEEE International Conference on Big Data, 2019, pp. 2587–2596.
[64] D.J. Solove, A taxonomy of privacy, Univ. Pa. Law Rev. 154 (3) (2005) 477–560.
[65] T.L. Morrison, Personal and professional boundary attitudes and effective group leadership in classrooms, J. Psychol. Interdiscip. Appl. 119 (2) (1985) 101–111.
[66] E. Karahanna, S.X. Xu, Y. Xu, et al., The needs–affordances–features perspective for the use of social media, MIS Q. 42 (3) (2018) 737–756.
[67] N. Zhang, C. Wang, Y. Xu, Privacy in online social networks, In Proceeding of International Conference on Information Systems, Shanghai, (2011) 2252.
[68] B. Ashforth, G. Kreiner, M. Fugate, All in a day's work: boundaries and micro role transitions, Acad. Manag. Rev. (25) (2000) 472–491.
[69] N.P. Rothbard, A. Ollier-Malaterre, Boundary management, in: The Oxford Handbook of Work and Family, Oxford University Press, 2016, pp. 109–122.
[70] E.E. Kossek, M.N. Ruderman, P.W. Braddy, et al., Work–nonwork boundary management profiles: a person-centered approach, J. Vocat. Behav. 81 (1) (2012) 112–128.
[71] I. Altman, The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding, Cole Publishing, CA: Monterey, 1975.
[72] S.Y. Margulis, Privacy as a social issue and behavioral concept, J. Soc. Issues 59 (2) (2003) 243–261.
[73] C.M. Angst, R. Agarwal, Adoption of electronic health records in the presence of privacy concerns: the elaboration likelihood model and individual persuasion, in: MIS Q., 33, 2009, pp. 339–370.
[74] Z. Jiang, C.S. Heng, B.C. Choi, Privacy concerns and privacy-protective behavior in synchronous online social interactions, Inf. Syst. Res. 24 (3) (2013) 579–595.
[75] J.Y. Son, S.S. Kim, Internet users' information privacy-protective responses: a taxonomy and a nomological model, MIS Q. 32 (3) (2008) 503–529.

[76] C.L. Anderson, R. Agarwal, The digitization of healthcare: boundary risks, emotion, and consumer willingness to disclose personal health information, Inf. Syst. Res. 22 (3) (2011) 469–490.
[77] P.B. Lowry, J. Cao, A. Everard, Privacy concerns versus desire for interpersonal awareness in driving the use of self-disclosure technologies: the case of instant messaging in two cultures, J. Manag. Inform. Syst. 27 (4) (2011) 163–200.
[78] J.M. Abowd, I.M. Schmutte, M I., An economic analysis of privacy protection and statistical accuracy as social choices, Am. Econ. Rev. 109 (1) (2019) 171–202.
[79] H. Xu, T. Dinev, J. Smith, et al., Information privacy concerns: linking individual perceptions with institutional privacy assurances, J. Assoc. Inf. Syst. 12 (12) (2011) 1.
[80] G. Bansal, D. Gefen, The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern, Eur. J. Inform. Syst. 24 (6) (2015) 624–644.
[81] H. Xu, H.H. Teo, B.C. Tan, et al., Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: a study of location-based services, Inf. Syst. Res. 23 (4) (2012) 1342–1363.
[82] V. Krishnan, S. Gupta, Appropriateness and impact of platform-based product development, Manag. Sci. 47 (1) (2001) 52–68.
[83] M. Muffatto, M. Roveda, Product architecture and platforms: a conceptual framework, Int. J. Technol. Manag. 24 (1) (2002) 1–16.
[84] S.C. Wheelwright, K.B. Clark, Revolutionizing Product Development: Quantum Leaps in Speed, Efficiency, and Quality, Simon and Schuster, 1992.
[85] C.Y. Baldwin, K.B. Clark, The architecture of participation: does code architecture mitigate free riding in the open source development model? Manag. Sci. 52 (7) (2006) 1116–1127.
[86] C.Y. Baldwin, C.J. Woodard, The architecture of platforms: a unified view, Platf. Mark. Innov. 32 (2009) 19–44.
[87] A. Ghazawneh, O. Henfridsson, Balancing platform control and external contribution in third-party development: the boundary resources model, Inf. Syst. J. 23 (2) (2013) 173–192.
[88] K.J. Boudreau, Let a thousand flowers bloom? An early look at large numbers of software App developers and patterns of innovation, Organ. Sci. 23 (5) (2012) 1409–1427.
[89] B. Remneland-Wikhamn, J. Ljungberg, M. Bergquist, et al., Open innovation, generativity and the supplier as peer: the case of iPhone and android, Int. J. Innov. Manag. 15 (1) (2011) 205–230.
[90] B. Eaton, S. Elaluf-Calderwood, C. Sørensen, et al., Distributed tuning of boundary resources, MIS Q. 39 (1) (2015) 217–244.
[91] Y. Qiu, I.H. Hann, A. Gopal, From invisible hand to visible hand: platform governance and institutional logic of independent mac developers, 2001-2012, Proceeding of the Thirty Fourth International Conference on Information Systems, Milan, 2013.
[92] Y. Qiu, A. Gopal, I.H. Hann, Logic pluralism in mobile platform ecosystems: a study of indie app developers on the iOS app store, Inf. Syst. Res. 28 (2) (2017) 225–249.
[93] M. Barrett, E. Oborn, W.J. Orlikowski, et al., Reconfiguring boundary relations: robotic innovations in pharmacy work, Organ. Sci. 23 (5) (2012) 1448–1466.
[94] A. Mohagheghzadeh, F. Svahn, Shifting design capability to third-party developers: an affordance perspective on platform boundary resources, Proceeding of the Twenty-second Americas Conference on Information Systems, San Diego, 2016.

Dr. Chong (Alex) Wang is an Associate Professor at the Peking University Guanghua School of Management. He holds a Ph.D. in Information Systems from Hong Kong University of Science and Technology Business School, an MSc in Finance from Tsinghua University, and a BS in Applied Mathematics from Peking University. Dr. Wang's research interests are on the impact of technology development on creating, disseminating, and processing information in the digital economy. His works study social media, online social networks, open innovations, matching in online platforms, privacy, and emerging FinTech applications.

Dr. Nan (Andy) Zhang is an Associate Professor at the School of Management of Harbin Institute of Technology. He holds a Ph.D. in Information Systems from Hong Kong University of Science and Technology Business School, an MSc in Telecommunications from University College London, and a BS in Computer Science from Dalian University of Technology. Dr. Zhang's research areas are technology adoption, information privacy and security. His work has been published in journals and conferences in both information systems and marketing.

Dr. Cong Wang is an Assistant Professor at the Peking University Guanghua School of Management. She received her Ph.D. from School of Economics and Management, Tsinghua University, China. Her research interest lies in the intersection data analytics, artificial intelligence and management information systems.