ISSN: 2688-9323

Research Review on Information Privacy

Xinlei Qi

Shanghai University, China

Abstract

Starting from the concept and dimension of information privacy, this paper explores the sources and scope of information privacy in depth, and uses the method of literature review to explain the definition of information privacy from the four perspectives of rights, goods, controls and status. In addition, the current research progress of information privacy is summarized and summarized from the two perspectives of research and impact research, which provides a theoretical reference for the research related to information privacy.

Keywords

Information Privacy; Theoretical Reference; Methods of Literature Review.

1. Introduction

In April 2021, the Facebook privacy disclosure incident of more than 533 million users caused a great stir. Sensitive information such as phone number, name, location and resume were published on hacker forums, which triggered strong public concern about the security of personal information on social media. As the carrier of information collection and processing between enterprises and users, the design and implementation of privacy policies are valued by both enterprises and users. How to design privacy policies can reduce users' privacy perception risks, enhance users' trust in enterprises, and further enhance users' disclosure behavior so that enterprises can use users' personal information reasonably is a problem that most enterprises must consider. Therefore, this study summarizes and summarizes the existing research on information privacy, and looks forward to making contributions to the research on Information Privacy.

2. The Concept of Information Privacy

The concept of information privacy is transformed from the concept of privacy, and as information technology continues to mature and develop, the research category of information privacy is continuously expanding, gradually becoming an important branch of the privacy concept[1]. The concept of privacy was first proposed by Clarke as a tetrad that distinguishes privacy into personal privacy (concerning the integrity of an individual's body), privacy of personal behavior, privacy of personal communication, and privacy of personal data[2]. Smith made an induction of privacy, arguing that privacy contains physical privacy and information privacy, which mainly involves individuals' physical access to the surrounding environment and private spaces, while information privacy involves the access to identifiable personal information[3]. Based on the above two studies, Belanger et al. respectively delineated the scope of physical privacy and information privacy, in which, information privacy contains individuals' communication privacy and data privacy [4].

The definition of information privacy has proved notoriously difficult to define in previous studies [1], because of its multiple levels of meaning, the definition of existing studies calling for information privacy needs to combine specific situations, unfolding from different levels according to the variation of research scenarios [3]. Several definitions comparing ripening are

ISSN: 2688-9323

articulated from four perspectives: entitlement, commodity, control, and state. In terms of a rights perspective, turn considers information privacy as the right of individuals to collect, store, process, disseminate and use their own information [5]. Based on European and American privacy protection laws and cases, Newman considers information privacy as the right of users' personal information to be forgotten in the Internet [6]. In terms of the goods perspective, Acquisti et al explored the role of public policy in protecting privacy in the information age, considering that privacy is a good, for example, many people can spend more money for the protection of privacy, such as paying a premium on purchasing goods at sites that protect privacy, and there are also many who disclose privacy with rewards, such as registering a certain app that will return or offer free members [7]. Focusing on the privacy concerns of mobile technology in the retail sector by addressing user privacy concerns in the way of information management and interactive management, Hoehle argues that information privacy is the process by which individuals cooperate to provide their own data for economic purposes and trade for the benefit of them [8]. In terms of control perspective, existing studies generally agree that information privacy is closely related to control. First defined information privacy from a control perspective and widely adopted by subsequent research, Westin et al., identified information privacy as the extent to which individuals, groups, or institutions ask themselves to decide when, how, and to whom their information is communicated to others [9]. Stone discussed the implications of organizational and social policies on personal information processing, arguing that information privacy is an individual's ability to control information about himself or herself [10]. Focusing on the impact of information privacy in the field of e-commerce on users' behavioral intentions, Malhotra et al., argue that information privacy is an individual's desire to control or influence the access and potential secondary use of personal data [11]. Belanger et al summarized information privacy research in the field of information systems, concluding that information privacy is a multi-level concept, and he defined information privacy as the person's desire to influence or control his or her own data [4].

Table 1. Representational definition of information privacy

Rerspective	Definition	Author (s)
Right	Information privacy is the right of individuals to collect, store, process, disseminate and use their own information	Turn (1985) [5]
	Information privacy is the right of personal information to be forgotten in the Internet	Newman (2015) [6]
Commodity	Information privacy is a commodity that is secured by paying money or sold for benefit	Acquisti (2015) [7]
	Information privacy is the ability of individuals to cooperate to provide their own data for economic purposes, to trade for benefit	Hoehle et al. (2019) [8]
Control	Information privacy is the extent to which individuals, groups, or institutions can decide when, how, and to whom their information will be communicated to others	Westin (1968) [9]
	Information privacy individuals' ability to control information about themselves	Stone et al. (1983) [10]
	Information privacy is the individual's desire to control or influence the access and potential secondary use of personal data	Malhotra et al. (2004) [11]
	Information privacy is the individual's desire to influence or control their own data	Belanger et al. (2011) [4]
State	Information privacy is the state of limited personal information that can be accessed	Cheng et al. (2021) [12]

ISSN: 2688-9323

In terms of state perspective, Cheng studied the application of AI in the puzzle scene, using coping theory and privacy computing theory, and analyzed the benefits and risks that passengers feel when disclosing personal information, defining information privacy as the state of limited personal information that can be accessed [12]. This paper combs out existing research for the definition of information privacy as shown in Table 1.

Since it is almost impossible to measure information privacy per se, and significant relationships rely more on cognitive and perceptual than rational evaluations [3], almost all empirical privacy research in the social sciences has relied on the measurement of some kind of privacy related agency, with a preponderance of studies using privacy concerns as a proxy variable. Existing research on the impact of information privacy contains mainly antecedent Research (inputting Research) and behavior / willingness Impact Research (outputting Research).

3. Research on the Antecedents of Information Privacy

In terms of antecedent research, Hong et al based their research framework on multidimensional development theory to summarize and induce the antecedent variables of information privacy from two directions, personal dimension and environmental dimension [13]. Miltgen et al., examining the core issue that people's privacy may be concerned when they are threatened, extracted independent variables of information privacy from personal, contextual and macro environmental dimensions, and explored the differences between groups in the perception of information privacy in different cultural contexts [14]. Therefore, based on the above perspective, this study induces the antecedent variables related to information privacy of existing literatures, which are summarized from two levels, the personal dimension and the environmental dimension.

3.1. Research on Antecedents of Information Privacy in Personal Dimension

In terms of the impact of personal dimensions on information privacy, existing studies mostly focus on the impact of personal characteristics on information privacy, typically such as the perception of information sensitivity, the experience of privacy violations and the experience of Internet privacy protection. Li Rui and others pay attention to users' perception of privacy sensitivity, establish a user tolerance scale for privacy disclosure, study the impact of information sensitivity, use sensitivity and receiver sensitivity on privacy disclosure tolerance, and conclude that users' privacy tolerance for information sensitivity and use sensitivity is very low, and there are also large differences between individuals. Wang et al. Conducted research on how to alleviate the privacy concerns of users who have experienced privacy violations. Based on the communication privacy management theory, they concluded that users' privacy self-efficacy, the effectiveness of perceived privacy policies and the effectiveness of perceived privacy protection technology will all affect consumers' privacy concerns [15]. Based on the multidimensional development theory, Hong and others believe that the impact of personal factors on users' information privacy can not be ignored. Privacy infringement experience, risk aversion personality, and the sensitivity of information required by the website have increased concerns about Internet privacy, while familiarity with government legislation and rich Internet knowledge have significantly reduced concerns about Internet privacy [16]. Miltgen et al. Explored the impact of age on information privacy concerns. Young people are more optimistic about personal data management than the elderly, and they have more confidence in legal protection and self-protection ability [14]. Korzaan and others believe that different personality traits have an important impact on privacy concerns. Based on the theory of five personality traits, they found that affinity personality is more likely to produce privacy concerns, while rational personality is highly related to privacy protection behavior [17].

ISSN: 2688-9323

3.2. Research on Antecedents of Information Privacy in Environmental Dimension

In terms of environmental dimension, most of the existing studies show differences in the performance of information privacy in different environments from the aspects of cultural differences, right distance, regulatory environment and industry self-discipline. Miltgen et al. Established focus groups in seven different European countries and believed that people from collectivist countries expressed more trust than people from individualist countries and were unwilling to disclose information [14]. Heng et al. Explored the impact of compensation, industry self-discipline and government regulation on consumer privacy computing based on LBS (location-based services), further studied the role of push-pull two information transmission mechanisms in the process of personal privacy decision-making, and believed that the way of information transmission should be combined with the specific environmental background. For example, in the scenario of push LBS, providing economic compensation is more important than pull lbs. In addition, privacy advocates and government legislators should not treat all types of LBS equally, but should specifically target specific types of services [18]. Milberg et al. Tested cross-cultural samples from 19 different countries and found that a country's supervision of enterprise information privacy management is affected by its cultural values and personal information privacy concerns [19]. Bellman et al. Revealed by investigating the national laws and regulations of 38 countries that the differences in Internet privacy concerns are significantly reflected in cultural differences. They mainly formulate privacy protection policies for different cultures [20].

4. Research on the Impact of Information Privacy

In terms of behavior / intention impact research, the existing research on information privacy impact behavior mainly includes the privacy computing behavior based on rational people and the privacy paradox behavior based on irrationality, in which the privacy computing behavior will lead to two different behavior outcomes of privacy protection and privacy disclosure.

4.1. Research on Privacy Calculus Behavior

In terms of privacy computing behavior, most scholars have tried to describe the decision-making process of user privacy through the calculation of the risks and benefits of privacy from a rational perspective, [21] and most studies have concluded that privacy concerns and privacy disclosure behaviors are highly correlated. [22] Privacy risk is defined as the extent to which people may experience potential losses when disclosing their personal information to a business or other organization [11]. Most studies concluded that privacy risks can create user privacy concerns, resulting in a reduction in users' willingness to disclose [23]. Privacy benefits are defined as the sum of beneficial outcomes such as the disclosure of personal information by users, including economic benefits, [24] personalization services[25] and the integration of social relationships. [26] Van et al. focus on the impact of information privacy on their willingness to participate in online transactions, and the results show that consumers' concerns about information privacy affect well-known merchants' risk perception, trust, and willingness to trade, but not lesser-known merchants. [27] Based on the privacy computing model, Stern et al. found that perceived risk and perceived benefit are important antecedent variables for self-disclosure, attitudes and subjective norms significantly affect the use of online social media, the use of privacy settings does not hinder privacy disclosure, and providing users with privacy protection tools can significantly improve user privacy disclosure [28].

4.2. Research on Privacy Protection Behavior

The above research is based on the privacy disclosure behavior from the perspective of privacy computing, and with the gradual increase in the user's emphasis on information privacy and

ISSN: 2688-9323

the enhancement of users' awareness of privacy precautions, there has been a protection and circumvention of information privacy. Wirtz et al. found that consumers who perceive a lack of business policies or government regulation will try to regain the balance of power through various responses, such as falsifying personal information, using privacy-enhancing technologies, and refusing to buy [29]. Users with high levels of privacy concerns are reluctant to share and disclose personal information, and will take measures to reduce the possibility of personal privacy disclosure, such as removing personal accounts from mailing lists and not providing personal information online. [17] Son et al. concept theory of planned behavior into the field of information privacy, believing that perceived fairness is the main factor leading to consumers' handling of information privacy differences, and developed a classification method for information privacy protection responses, including information provision (refusal to provide information, misrepresentation), private action (deletion of personal information, negative evaluation) and public action (direct complaints to network companies, indirect complaints to third-party organizations), and privacy concerns affect all categories of protection responses (i.e., information provision, private action, and public action). Perceived equity only affects the provision of information, while social interests only affect public action[30].

4.3. Research on Privacy Paradox Behavior

Although the existing studies have reached a consensus on the research framework of privacy computing, there are still some studies that doubt this method. Many studies show that users are not completely rational when privacy is disclosed, and users' information privacy behavior may completely deviate from the interpretation scope of privacy computing theory, showing many irrational privacy paradoxes [31,32]. The generation of the privacy paradox phenomenon is that people have uncertainty about the consequences of privacy disclosure, leading to their inability to clearly understand the preferences of the consequences of privacy disclosure, and the behavior of privacy disclosure will show significant differences in different situations [7]. The privacy behaviors of users do not completely match their expectations, and even show great differences. In some cases, users even completely ignore the awareness of privacy protection, reduce privacy concerns and disclose personal information without reservation [33]. Norberg and others believe that background factors are the main reasons for the difference between disclosure intention and disclosure behavior, such as physical environment, social factors reflecting the relationship between individuals and individuals or institutions collecting information, and cognitive factors [34]. Adjerid et al. Also paid attention to the difference between the willingness to disclose privacy and the privacy behavior before. The research concluded that consumers would overestimate their response to the willingness to disclose and underestimate their response to behavioral factors. However, neither the objective risk perception based on the willingness to disclose nor the relative risk perception based on the disclosure behavior will affect consumers' privacy decisions [35]. It shows that when the user is not clear about the information disclosure scenario, the user's disclosure intention and disclosure behavior will show great differences, but on the premise of determining the disclosure scenario, the user's disclosure intention and behavior are basically the same.

5. Conclusion

This study explains the definition of information privacy from the perspectives of rights, commodities, controls and status, and describes the progress of information privacy research in detail based on the analysis methods of the literature review from the perspectives of antecedent research and outcome research. The research results show that in terms of antecedent research, the main focus is on the impact of individual dimensions and environmental dimensions on the user's information privacy perception, and in the result

ISSN: 2688-9323

research, it also shows the privacy computing behavior based on the assumption of rational people, the privacy paradox behavior based on the assumption of irrational people, and the privacy protection behavior based on the awareness of prevention.

References

[1] Finn R L, Wright D, Friedewald M: Seven types of privacy, European data protection: Coming of age, 2013: 3-32.

[2] Clarke R. Internet privacy concerns confirm the case for intervention[J]. Communications of the ACM, 1999, 42(2): 60-67.

[3] Smith H J, Dinev T, Xu H J M Q. Information privacy research: An interdisciplinary review[J]. MIS Quarterly, 2011: 989-1015.

[4] Belanger F, Crossler R E. Privacy in the digital age: A review of information privacy research in information systems[J]. MIS Quarterly, 2011, 35: 1017-1041.

[5] Turn R. Privacy protection[J]. Annual review of information science and technology, 1985, 20: 27-50.

[6] Newman Abraham L. What the “right to be forgotten” means for privacy in a digital age[J]. Science, 2015, 347(6221): 507-508.

[7] Acquisti A, Brandimarte L, Loewenstein G. Privacy and human behavior in the age of information[J]. Science (New York, N.Y.), 2015, 347: 509-14.

[8] Hoehle H, Aloysius J A, Goodarzi S, et al. A nomological network of customers’ privacy perceptions: Linking artifact design to shopping efficiency[J]. European Journal of Information Systems, 2019, 28(1): 91-113.

[9] Westin A F. Privacy and freedom[J]. Michigan Law Review, 1968, 66(5).

[10] Stone E, Gueutal H, Gardner D, et al. A field experiment comparing information-privacy values, beliefs, and attitudes across several types of organizations[J]. Journal of Applied Psychology, 1983, 68: 459-468.

[11] Malhotra N K, Kim S S, Agarwal J. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model[J]. Information Systems Research, 2004, 15(4): 336-355.

[12] Cheng X, Su L, Luo X, et al. The good, the bad, and the ugly: Impact of analytics and artificial intelligence-enabled personal information collection on privacy and participation in ridesharing[J]. European Journal of Information Systems, 2021.

[13] Hong W, Thong J Y L. Internet privacy concerns: An integrated conceptualization and four empirical studies[J]. Mis Quarterly, 2013, 37(1): 275-+.

[14] Miltgen C L, Peyrat-Guillard D. Cultural and generational influences on privacy concerns: A qualitative study in seven european countries[J]. European Journal of Information Systems, 2019, 23(2): 103-125.

[15] Wang L, Sun Z, Dai X, et al. Retaining users after privacy invasions: The roles of institutional privacy assurances and threat-coping appraisal in mitigating privacy concerns[J]. Information Technology & People, 2019, ahead-of-print.

[16] Hong W, Chan F K Y, Thong J Y L. Drivers and inhibitors of internet privacy concern: A multidimensional development theory perspective[J]. Journal of Business Ethics, 2021, 168(3): 539-564.

[17] Korzaan M L, Boswell K T. The influence of personality traits and information privacy concerns on behavioral intentions[J]. Journal of Computer Information Systems, 2008, 48(4): 15-24.

[18] Xu H, Teo H-H, Tan B C Y, et al. The role of push-pull technology in privacy calculus: The case of location-based services[J]. Journal of Management Information Systems, 2009, 26(3): 135-174.

[19] Milberg S J, Smith H J, Burke S J. Information privacy: Corporate management and national regulation[J]. Organization Science, 2000, 11(1): 35-57.

ISSN: 2688-9323

[20] Bellman S, Johnson E J, Kobrin S J, et al. International differences in information privacy concerns: A global survey of consumers[J]. The Information Society, 2004, 20(5): 313-324.

[21] Culnan M J, Bies R J. Consumer privacy: Balancing economic and justice considerations[J]. Journal of Social Issues, 2003, 59(2).

[22] Phelps J, Nowak G, Ferrell E. Privacy concerns and consumer willingness to provide personal information[J]. Journal of Public Policy & Marketing, 2000, 19(1): 27-41.

[23] Dinev T, Hart P. An extended privacy calculus model for e-commerce transactions[J]. Information Systems Research, 2006, 17(1): 61–80.

[24] Hann I-H, Hui K-L, Lee S-Y T, et al. Overcoming online information privacy concerns: An information-processing theory approach[J]. Journal of management information systems, 2007, 24(2): 13-42.

[25] Zeng F, Ye Q, Yang Z, et al. Which privacy policy works, privacy assurance or personalization declaration? An investigation of privacy policies and privacy concerns[J]. Journal of Business Ethics, 2022, 176(4): 781-798.

[26] Wang T, Duong T D, Chen C C. Intention to disclose personal information via mobile applications: A privacy calculus perspective[J]. International Journal of Information Management, 2016, 36(4): 531-542.

[27] Van Slyke C, Shim J, Johnson R, et al. Concern for information privacy and online consumer purchasing[J]. J. AIS, 2006, 7.

[28] Stern T, Salb D. Examining online social network use and its effect on the use of privacy settings and profile disclosure[J]. Bulletin of Science, Technology & Society, 2015, 35(1-2): 25-34.

[29] Wirtz J, Lwin M, Williams J. Causes and consequences of consumer online privacy concern[J]. International Journal of Service Industry Management, 2007, 18: 326-348.

[30] Son J-Y, Kim S S. Internet users' information privacy-protective responses: A taxonomy and a nomological model[J]. MIS Quarterly, 2008, 32(3): 503-529.

[31] Acquisti A, Grossklags J. Privacy and rationality in individual decision making[J]. IEEE Security & Privacy, 2005, 3(1): 26-33.

[32] Jensen C, Potts C, Jensen C. Privacy practices of internet users: Self-reports versus observed behavior[J]. International Journal of Human-Computer Studies, 2005, 63(1): 203-227.

[33] Berendt B, Günther O, Spiekermann S. Privacy in e-commerce: Stated preferences vs. Actual behavior[J]. Communications of the ACM, 2005, 48(4): 101–106.

[34] Norberg P A, Horne D R, Horne D A. The privacy paradox: Personal information disclosure intentions versus behaviors[J]. The Journal of Consumer Affairs, 2007, 41(1): 100-126.

[35] Adjerid I, Peer E, Acquisti A. Beyond the privacy paradox: Objective versus relative risk in privacy decision making[J]. MIS Quarterly, 2018, 42: 465-488.