Review of Research on Privacy Decision Making from a Time Perspective

Zhuoran Jiang
University of Texas at Austin
Zhuoran.Jiang@mccombs.utexas.edu

Sirkka L. Jarvenpaa
University of Texas at Austin
Sirkka.Jarvenpaa@mccombs.utexas.edu

Abstract

Managing privacy is a process in which people continuously negotiate the boundaries of their personal space. Time is embedded in and influences this continuous negotiation. Digital technologies increasingly incorporate temporal elements, such as allowing users to define the expiration date of social network postings. Yet, researchers have not systematically examined the effects of temporal elements in privacy decision making. In this paper, we review how existing information privacy research has related to time in terms of three dimensions: duration, timing, and past, present, and future modalities. Our findings suggest that 1) duration has a negative influence on information disclosure; 2) timing, in the form of personal and external events, influences how people make privacy decisions; and 3) sensemaking that involves prior experience and planning for the future affect privacy decisions. We discuss how privacy decision making frameworks need to be adjusted to account for a time perspective.

1. Introduction

Users exchange personal information in return for benefits, such as financial rewards, personalization, and online social identity on a variety of digital technologies [1]. This communication about oneself to others is commonly understood as information disclosure. Information disclosure from users is the major source of data that supports many digital business models. For instance, smart speakers (e.g., Alexa) customize the search results based on users' profile and historical search data. Social networking sites (SNSs) personalize advertisements on the basis of users' disclosed information.

Greater information disclosure leads to information privacy threats such as identity theft and cyberstalking. Individuals become more hesitant to disclose their personal data. Studies have found that users delete online information, provide fake information, and even abandon technology [2]. Companies need to develop strategies to balance their objectives of encouraging information disclosure and protecting users' privacy to achieve business viability and sustainability.

Such strategies include implementing temporal elements in digital technologies. For example, WeChat, a popular social media application in China, allows users to define the length of time for which their posts are viewable by friends (e.g., "Last 3 days"). Similarly, smart speaker Alexa can set up auto-deletion of voice recordings at 3-month or 18-month marks. Facebook Timeline organizes a user's activities in a reverse-chronological manner that allows revisiting of the "past" of a person. Twitter provides "Trendings" to let users stay updated with the latest news and stories.

Although companies are offering temporal "solutions" to users, the literature contains little systematic understanding of their effects in relation to information disclosure and privacy decision making. Neither does it include a review of what is already known about interfaces and tools that help users to negotiate different temporal aspects of information disclosure, such as long-term presentation of historical data, duration of public postings, and timing of disclosure. A review of the literature can shed light on whether such temporal elements advance companies' business goals of mitigating users' privacy concerns while encouraging users' information disclosure.

We carry out a review of research on privacy and information disclosure from a time perspective. The research objectives of this paper are threefold: 1) to review how existing literature has discussed time in the context of information privacy; 2) to explore privacy-protective design recommendations that incorporate time elements; and 3) to propose new research avenues for privacy studies from a temporal perspective.

2. Conceptual Background

2.1. Privacy decision making and information disclosure

Information privacy is defined as individuals' ability to control data about themselves [3]. Scholarly work has examined the relationship between privacy concerns and other constructs, and developed the Antecedent–Privacy Concern–Outcome (APCO) model

URI: https://hdl.handle.net/10125/71421
978-0-9981331-4-0

[1], [4], [5]. Examples of antecedents of privacy concerns include privacy experiences, privacy awareness, personality differences, demographic differences, culture/climate and so on [1]. The widely studied outcomes include individuals' information disclosure intentions and behaviors [5].

Online users disclose their personal information every day – for example, when they register for an e-commerce account with their phone number. One consistent finding is that although individuals report strong privacy concerns, they still keep disclosing personal information online. This discrepancy between the stated privacy concern and the actual disclosure behavior is called the privacy paradox [6]. The privacy paradox has been studied by researchers mainly from two perspectives: normative and behavioral. The normative perspective focuses on elements that influence the objective benefits and costs of information disclosure. It has advanced the privacy calculus model, which states that people would weigh the perceived benefits and perceived risks of information disclosure to make privacy decisions [7]. The privacy calculus model continues to be actively researched and referenced in studies of privacy decision making (e.g., see [8]–[10]). The behavioral perspective integrates principles from behavioral economics and psychology, and believes that privacy decision making is influenced by heuristics and biases such as herding and anchoring effects [4], [11]. These behavioral factors are independent from the objective benefit-risk trade-offs and help explain deviations from the normative accounts of user privacy decisions [12].

2.2. Time and time dimensions

In the studies of physical privacy, managing privacy is viewed as a dialectic process in which people can continuously negotiate and manage the boundary of their personal space [13], [14]. Similarly, in information privacy, privacy preferences and judgments are assumed to be relative and malleable in nature [12]. We posit that a concept of time is implicitly embedded in the continuous negotiation of information privacy. To fully understand information disclosure behavior, research needs to account for time.

Time is an integral aspect of human lives. Time provides standards for measurement, coordination, regulation, and control [15]. We adopt Berends and Antonacopoulou's [16] three dimensions of time, which were based on Adam's seminal work on timescapes [17]. The three dimensions allow us to begin to understand the temporal effects in both the normative and behavioral research streams.

The first dimension is duration, which describes the degree of expansion in time [18]. In information privacy and disclosure, duration manifests itself in different ways, such as how long an individual has used Facebook and how long a selfie has been shared. Users' privacy concerns and willingness to disclose information might change over time.

The second dimension, timing, is about when events happen, or when actions are undertaken. Timing can be indicated by clock and calendars (clock time) or by the occurrence of certain events (event time) [16]. In its relation to information privacy and disclosure, timing is manifested in many different ways, such as an emotional moment that triggers disclosure or a data breach news that prevent sharing information.

The third dimension of time – the temporal modalities of past, present, and future – is also referred to as "inner time" [19]. Individuals can experience their past and future in a cognitive process. This dimension helps explain people's present privacy decision making by answering questions such as these: How will prior privacy violation experience affect disclosure behavior? How will identity management goal influence disclosure decision?

3. Methodology

We started our literature search in the AIS "basket of eight" information systems (IS) journals and two computer science (CS) databases, ACM Digital Library and IEEE Xplore. We searched for articles published since 2000 which included the combination of keywords "privacy" and "time" in the abstracts (in the full text if abstract option was not available). This gave us 1915 articles for initial screening. We then scanned the titles and abstracts of each article and only included articles that met the following criteria: 1) focused on privacy decision making in a digital technology setting; 2) explicitly mentioned one or more aspects of time that map to duration, timing, or past-present-future modalities. 1907 records were excluded and only 8 full-text articles were identified as relevant after the initial screening.

To broaden the search, we adopted a backward and forward approach [20]. We went backward by reviewing the citations in the 8 articles. We then went forward by using Google Scholar to identify papers that have cited the 8 articles, as well as those deemed relevant in the backward search. When we found new relevant articles, we again examined them backward and forward. This iterative process produced 29 additional papers. In total, 37 papers were included for review (indicated with asterisks in the references).

We adopted an abductive method to code the papers as this is an explorative research aiming at inspecting an unexamined area; via juxtaposing deductive and inductive approaches, we identified new

constructs and relationships [21]. In terms of deduction, we started with the three time dimensions defined in the literature. Inductively, we abstracted excerpts in each paper that matched these dimensions ("quote") and then developed more-refined constructs of these dimensions describing how each dimension was manifested in these excerpts ("new constructs"). Then inductively, we identified "mechanisms" that can explain how these new constructs affected privacy decision making, such as by "*decreasing content relevance*". We also summarized the technology context of each paper ("context") and abstracted recommendations for time-related interface design when they were offered. The first author and two research assistants first coded the articles independently, then compared codes and addressed any discrepancy through discussion. The coding results were documented as a concept matrix [20] grouped by dimension, new construct, and mechanism. Table 1 presents examples of the coding results.

Table 1. Coding results with sample quotes

	New Constructs	Mechanisms	Papers and Context	Quote (example)
Duration	Information age	Decreasing relevance	Social media: [22]–[30]; Cloud storage: [31] [32] [33]; Smart device: [34]	"I don't need [that photo] anymore and that folder is full of junk photos". [31]
		Increasing visibility	Social media: [26], [28], [30], [35]; Software system: [36]	"[I tweeted] something sexual and my [T]witter at the time was public, so I freaked out when I saw that my brother's screen name popped up on Recommended Twitter." [35]
	Technology age	Accumulating knowledge / awareness	Social media: [37]–[39]; Smart device: [40]–[43]	This [privacy] concern stems from increased awareness [of potential threats]; recent smart speaker mishaps, erroneous code used in them… have led to an increasing [privacy] concern... [40]
	User age	Increasing attention to private life	Social media: [38], [44]; General: [45]	[O]lder people are more privacy-protective than younger people…[T]he increases in consumer privacy concerns may be explained by a widening in scope of the contexts in which privacy is relevant. [45]
Timing	Personal event	Major life changes	Social media: [29], [30], [46]	The occurrence of life changes…reduces the participants' willingness to share information that was published before the change occurred. [30]
		Emotional experience	Social media: [22], [24], [35], [47]	"I was so frustrated at the time, posting a status about it was a slight relief from the situation…" [24]
	External event	Reputational challenges	Social media: [48]; Smart device: [49]; General: [50]	[P]articipants' concerns about the speaker tended to intensify if they saw negative news [related to the device]. [49]
		Technological improvements	Social media: [46]; Software system: [51]–[53]	"The [privacy warning] icons help me gauge which permissions are influencing each risk level, and that helps me manage which permissions to accept or reject." [51]
		Relentless & sensational reporting	Social media: [46]; Smart device: [54]	[E]lections and news about data breaches were the most frequently mentioned global events motivating changes. [46]
Temporal Modality	Reflection	Prior experience	Social media: [55]; Smart device: [54]; Recommender system: [56]; General: [14]	[N]egative prior experience might make people more cautious about the system's access and use of their data. [56]
	Planning	Identity management	Social media: [24][55]; Cloud storage: [57]	Users are concerned about information revelation because they fear that a future employer might look at their profiles. [55]
		Reminiscence	Social media: [24]	"[A] lot of times Facebook is the way that I remember stuff … And I like to go back and see how … my silly friends and I were, back in the day." [24]

4. Findings

Our findings present the new constructs that provide more granular manifestation of the temporal dimensions along with their mechanisms (in *italics*) that explain how time renders differences in privacy decision making. We report on design elements that seem to recognize the role of time in mitigating privacy concerns and encouraging information disclosure.

4.1. Finding I: time as duration – age of information, technology, and user

Duration describes the degree of expansion in time [18]. In information privacy, duration has been manifested in three ways: information age, technology age, and user age. Information age refers to the length of time that content has been disclosed. Technology age represents the length of time a technology has been available to and used by an individual. User age refers to an individual's chronological age. The review suggests that privacy concerns over disclosed data increase with the passage of time, both in short and long durations. For example, information age is present in the time span of a Facebook post: The longer the post has been disclosed, the older the information. A poster's willingness to share that information has been found to decline as the information ages because of the *decreasing content relevance*.

Although users might have different perceptions of the recency of disclosed information, they tend to believe that recent content is more relevant to both self-representation and viewers' interests [23], [24], [26], [29]. One Facebook user said "[The post] appealed to the nerd in me, but a month later was no longer fresh" [23]. Decrease in relevance can result from the decline in the contextual integrity of information, which describes the extent to which the information is interpreted in its original context [58], [59]. As time passes, the original context in which the information disclosure took place shifts, and the contextual integrity of the information decreases. The information becomes irrelevant in the changed context and can be misinterpreted. This will reduce the accuracy of information and can harm one's privacy [25], [28]. Therefore, an individual's privacy concern tends to increase, and disclosure willingness tends to decline over time.

Digital technologies vary in handling information age. Contrary to the automatic archiving feature on Facebook, Snapchat adopts auto deletion mechanism. This ephemerality element prevents the accumulation of older and potentially embarrassing content for users [27]. A study finds that with cloud technologies, such as Dropbox and Google Drive, users no longer remember or recognize the value of many old files as time passes: "I don't need [that photo] anymore, and that folder is full of junk photos" [31].

Besides changing relevance, information age can influence dissemination and hence lead to larger viewing audiences and *increasing content visibility*. The range of viewers can extend as technology users grant access permissions to more friends, many of whom are just virtual friends but strangers in real life. The increasing numbers of viewers and the possibility of unintended disclosure can lead to more cautious disclosure from users. In addition, information that is disclosed can later inspire regret and then be deleted [23], [28], [29], [31]. For example, on SNSs, user-generated posts can be viewed by more observers as time passes, which can result in unintended disclosure. One participant described how she was afraid that her sensitive tweet might be seen by her brother: "[I tweeted] something sexual and my [T]witter at the time was public, so I freaked out when I saw that my brother's screen name popped up on Recommended Twitter" [35].

In addition to information age, the reviewed papers consider the age of technology. Technology age refers to the length of time a technology has been available to and used by the user; for example, a household member began using a smart speaker at home three years ago. The review shows that older technology is associated with stronger privacy concerns as users *accumulate knowledge/awareness of the technology.* As individuals become more familiar with the technology, they accumulate awareness of its potential privacy threats and vulnerabilities. As a result, users are more vigilant about fraudulent and maladaptive behaviors and more aware of targeted advertising practices; they become more strategic in their disclosure of information [37], [38], [43]. When people have a growing awareness of the risks associated with disclosing personal information, they adjust their privacy settings [39]. People become increasingly private even when privacy is not explicitly warranted [45]. Users' privacy concerns become stronger as they realize how insufficient the privacy protections from technologies can be, as well as when they realize the possible malfunctions of the technologies [40]. A study on smart speaker uses finds that privacy concerns were expressed due to accidental activations of the devices: "There were times when the speaker would activate without me saying the wake word. This was a bit odd and it did leave me a bit uneasy" [41].

Finally, age of a user refers to the length thus far of a person's lived life. Young people are found to be less concerned about their privacy because they perceive they have little to hide from the public,

whereas older people realize their lapsed time has made them more vulnerable and have learned to strategically control their information disclosure to reduce their vulnerability [38], [44]. Individual differences in privacy expectations come about at different ages because of *increasing attention to one's private life*. In one study, a participant responded, "I know at school you're like 'whatever,' it doesn't matter and it won't come back to haunt me; but when you go through uni and getting jobs, you think about it a lot more" [38]. Another study concluded that "[t]he increases in consumer privacy concerns may be explained by a widening in scope of the contexts in which privacy is relevant" [45].

The "duration" risks of information, technology, and individual ages have not gone unnoticed in terms of interface design. Several papers propose design alternatives that can afford users control over older and irrelevant information that can negatively influence their identity management. For example, one interface element is to establish an expiration date for information [29], [30], [61]. Users can customize, at the point of disclosure, when their information will be revoked or destroyed [32], [33]. Alternatively, service providers can set a standard expiration date. One study finds that more than 50% of the sample would consider certain information irrelevant two years after its initial publication [30]. Additionally, SNSs can implement an ephemerality mechanism that supports default deletion to avoid long-term exhibition of content, similar to Snapchat [27]. Another design element is simply to obscure older information while emphasizing the existence of more recent content [25], [26], [55]. Older information can be moved from public or group access to private archives [24].

4.2. Finding II: time as timing – occurrence of personal and external events

Timing refers to when events happen or when actions are undertaken [16]. In the reviewed papers, timing dimension has been manifested as two types of events: personal and external. Unlike the effects of duration, which were somewhat homogenous on information disclosure, the effects of timing showed heterogeneity in impacting privacy decision making.

Personal events are occasions of or affecting a particular user. Personal events include *major life changes*, such as moving to a new city, graduation, childbirth, and career changes. These life events could lead to changes in users' social circles and thus influence their privacy decision making. Participants in one study reported a reduced willingness to share information that was published before changes occurred in certain social relationships [30]. For instance, colleagues in a law firm were not deemed an appropriate audience for college-era party photos [46]. Personal events can trigger a strong *emotional experience* that encourages disclosure [22]. But disclosure of highly self-expressive or offensive content might later be regretted [24], [35], [47]. Such findings indicate that timing can influence users' willingness to disclose information but also can increase subsequent regrets. For example, one user described how an emotional expression could be improper afterwards: "I was so frustrated at the time, posting a status about it was a slight relief from the situation…. [Later on,] I thought my status may have come off as a bit whiney or condescending…" [24].

External events are occasions that relate to or arise from the surroundings of an individual, such as service providers or society. Events of a specific technology company can affect privacy decision making in the form of *reputational challenges* [50]. For example, users' trust in and privacy concerns of a platform can differ significantly after an accidental data breach on the platform [48]. People's privacy concerns will intensify when they encounter negative news about device manufacturers, related either to data use or to device performance [49]. Moreover, company-level events can impact disclosure behavior via *technological improvements*. For example, Facebook users claimed they would use privacy-protecting features on the platform if they were available, such as the "privacy checkup" tool and the "limit past audience" tool [46]. Mobile phone users report that they may change their privacy attitudes and stop using applications if they are prompted with worrisome privacy notices [51]–[53]. Additionally, external events can play a role at the social level, via *relentless and sensational reporting* (e.g., elections) [46], [62]. To illustrate, the Facebook–Cambridge Analytica scandal, in which millions of Facebook users' personal data was collected and sold for political purposes without consent, was a society-wide controversy that affected the trust among Internet users broadly, regardless of whether they were Facebook users [54].

For interface designers, timing presents challenges in managing the uncertainty around events. Interface designers search for design solutions that can take into account and predict the timing of events and the related information disclosure behavior. Designers are interested in attenuating individuals' current emotional states that later heighten privacy concerns; the goal is to curtail regrets that can lead to deletions of content. For example, two papers propose content-based sentiment detection mechanisms [35], [47]; the proposals are based on evidence that the timing of emotional experience can influence users' willingness to disclose. If users receive an alert during a time of

strong negative emotions, this alert can help users to self-censor and to reduce postings that they later regret and delete. Because negative emotions often compromise users' self-censoring capability, the systems themselves might need to do more than alert the user. One recommendation is to mark the negative content with visual icons or texts [35].

4.3. Finding III: time as past, present, and future modalities – reflection and planning

Time has *past, present, and future modalities*. This dimension is about people's subjective experiences of time [16]. To illustrate, individuals' current privacy decision making can be the result of their reflection of the past and planning for the future. On the one hand, people learn from *prior experience*. They might follow in their pattern of previous responses, or they might adjust their reactions if they were not satisfied with the previous outcome [14]. Individuals who have experienced privacy invasions express higher privacy concerns and exercise more caution regarding the access and use of data [54], [56]. For example, when making financial transactions online, people might draw on their past experience with other merchandisers to decide whether they think saving their mobile phone number for future use is safe. If they start to receive phone calls from unknown advertisers after disclosing the information, they will adjust their behavior.

On the other hand, many people plan for the future. Individuals take a prospective approach and are concerned about the influence of current privacy decisions on future action [14]. They might decide to disclose or not to disclose information to satisfy certain needs. One task that involves future planning and has become more critical in recent years is *identity management*. For example, for SNS users, public profiles can reflect their self-image, affect how others judge a person, and subsequently influence their long-term reputation [24], [55]. Some SNS users might retain a picture of themselves attending an MIS conference on SNSs because it reveals their enthusiasm for their work in academia. However, inappropriate content on SNSs can adversely affect individuals' identity construction. Identity management relies on a *future* orientation; a more complex use of time modalities is relevant in *reminiscence*. Digital technologies, such as Facebook Timeline, can act as the curator of memories [24].

Considering the temporal modalities of past, present, and future, researchers propose two distinct mindsets in data management: retrospective and prospective. Retrospective views manage digital items based on past use, while prospective views manage decisions based on future use. Most traditional management tools are retrospective, but one study suggests that prospective decision making also could help in preventing sensitive data leakages [57]. The study proposes a mobile application that enables users to decide, prospectively, what to do with cloud data in the future. One example was to delete selfies if the available storage space dropped below a preset level. This prospective approach considers potential future uses of data to make keeping or discarding decisions. However, tensions can arise. Because individuals have long-term needs related to reminiscence, old data might seem irrelevant in that they may raise greater privacy concerns, but they nevertheless act as media of recollection as time passes. Platforms such as SNSs thus should provide a separate region for historical data curation in addition to the public exhibition space [24].

4.4. Finding IV – time in technologies

The reviewed papers addressed varied technologies, including social media, smart devices, cloud storage, and various software systems. Although SNSs dominate in terms of the numbers of studies, our review does not find notable systematic differences across technologies. However, this neglect of systematic distinctions may occur because comparative studies looking at different technologies and their temporal elements are currently lacking. Hence, we can only speculate about differences across technologies. For example, one difference potentially arises from the diverse range of recipients and holders of information disclosed on different technologies. Data disclosed on smart devices (e.g., smart speakers, activity sensors) become available to the manufacturers or service providers of these devices; on social media, posts are viewable to both friends and strangers; emails and cloud documents are usually accessed by and available to people within professional networks. Different technologies produce different audiences and involve different durations and timings of disclosed information. Some of these differences may affect how individuals perceive the relationship between time dimensions and privacy.

5. Implications for Research and Practice

5.1. Theoretical implications

The review findings introduce new constructs and mechanisms and have implications for current privacy decision-making research. The APCO model on privacy concerns [4], though actively researched and referenced in privacy decision-making studies, focuses primarily on the factors that influence the initial

privacy decision making. This review from a time perspective suggests that examining the initial privacy decisions is not sufficient to understand information disclosure. The three time dimensions are considered as static factors but can indicate implicit changes in privacy decision making. For example, duration indicates a length of time in which information age, technology age, or user age can increase, leading to changes in one's information disclosure behavior.

First, the findings on duration demonstrate that people's intent to disclose can decrease as data, technologies, or individuals age. This raises questions about the widely accepted privacy calculus model. Studies adopting this model consider perceived benefits and perceived risks and costs simultaneously and only once (e.g., see [8]–[10]). The implication of our findings is that both perceived benefits and perceived risks are subject to changes over time. The privacy calculus model needs to be adjusted to reflect a more process-oriented perspective that accounts for change. Specifically, the privacy calculus model needs to be extended to clarify the time span in which the perceived benefits and risks are assessed. For example, the perceived benefit of self-expression on SNS [8] can diminish because the relevance of the content declines over the information age. The perceived risk related to health information sensitivity on healthcare-related wearable devices [10] can increase as technology ages because individuals become more aware of possible risks from improper use of data.

This extension of time span is consistent with the behavioral perspective. According to the hyperbolic discounting theory [63], short-term gains tend to be assigned greater weight compared with long-term losses. If the time span of information disclosure is relatively short, users pursue immediate gratification and ignore potential privacy loss in the future. If users assess the privacy issues related to disclosure within a longer time span, such as a year, then both perceived benefits and perceived risks become relatively distant. The privacy calculus is affected because the perceived privacy risks can be just as or more salient compared with the perceived benefits.

The broader implication for future research is that it needs to incorporate the time span element into privacy decision making frameworks. Modified frameworks can help address research questions, such as how perceived benefits and perceived risks of information disclosure change over time. Additional questions include: Do these changes have a significant effect on individuals' disclosure behavior? How can interface design help to preserve perceived benefits and mitigate perceived risks in the long run?

Second, the findings on timing show that the occurrence of personal and external events can make a difference in people's disclosure intentions and behavior. Timing influences how individuals interact with events [18]. Timing complicates the normative approach to understanding privacy decision making. The complication comes from the different weights that people allocate to normative factors under different circumstances. For example, personality difference is one antecedent in the APCO model. Xu [64] studies the differences in privacy attitudes toward location-based services (LBS) between independent people and interdependent people. If timing factors are incorporated, however, results can be different. For instance, negative emotional events might cause independent people to assign less value to privacy and display more favorable attitudes to LBS.

More broadly, the findings on timing imply that no universal framework can contain every type of antecedent of privacy decision making because the timing keeps changing the relevance of a wide range of antecedents in different scenarios. Future research might study the following questions: How does the occurrence of personal and external events moderate the effects of antecedents on privacy decision making? Which types of events have more influence on individuals' privacy decision making? How does interface design help in managing incongruences between disclosure intent and behavior due to timing?

Third, the findings on past, present, and future modalities suggest that privacy decision making is the result of sensemaking and planning. This time dimension has implications especially on the behavioral perspective of privacy decision making. The reason is that sensemaking is influenced by prior experience and by cognitive short-cuts, such as herding and anchoring effects [11]. Sensemaking can be, and often is, subject to individual differences, which raises questions about how to capture similarities and differences in individual responses to interface design tools that nudge people to disclose information. From a prospective perspective, researchers have studied how people's need for long-term identity management can influence their disclosure behavior (e.g., see [65]). However, they have not yet explored how people deal with conflicts related to long-term needs. To address this gap, future research might study how individuals balance their needs for long-term self-representation and for reminiscence.

5.2. Practical implications

The review findings suggest that, to improve understanding of users' privacy decision making, factors related to and expressing time have to be explicitly considered. Improved understanding can help companies design interface elements that not only

protect users' privacy but also allow users to enjoy personalization and other benefits that accrue from information disclosure. For companies relying on digital technologies for their business models, the negative relationship between duration and information disclosure behavior suggests that technologies need to be designed to help users manage duration. Without such design elements, people become less willing over time to share information or to use technologies. The uncertainty in the timing dimension indicates that digital technologies need to become smarter at predicting emotions and guiding or managing user disclosure behavior. Technologies that adopt sentiment detection tools can help users to self-censor and avoid storing data that users might soon want to delete. Technologies also need to be more responsive to users' reactions to external events, such as elections and data breach news, and to plan for changes in users' behavior such as disclosure frequency and amount. In terms of past, present, and future modalities, digital technologies can provide users with separate spaces for long-term self-presentation and reminiscence to avoid potential tensions.

The time perspective also has implications for policy makers. For example, policy makers need to consider the longitudinal management of personal data collected by digital companies. Is it proper to store and use historical data of users apart from the data's original temporal context? While erasing a person's past immoral behavior online can mislead others and disguise ongoing risks related to the person's moral choices, when and how should online users be guaranteed the right to be forgotten?

This review has several limitations. First, we abstracted the mechanisms (in *italics* in Findings) of how time affects privacy decision making mostly from qualitative papers in our review. Although the reviewed papers consist of a mixed set of qualitative and quantitative studies, the conceptual (e.g., see [53]) or descriptive studies based on interviews (e.g., see [49]) are more explanatory and provide richer theoretical grounds. Hence the mechanisms identified, and the significance of their effects will need empirical examination. Second, our research focuses on the generic role of time in information disclosure on digital technologies, thus we do not consider the potential differences across varied technologies. Third, the three time dimensions we used in the content analysis take the users' point of view. Future research can consider how time concepts can be structured and understood from the technology vendors' point of view to make themselves more privacy-protective.

Acknowledgements. We thank Dheemant Dammanna and Vennela Gajjala for their valuable help as undergraduate research assistants in this project.

6. References

[1] H. J. Smith, T. Dinev, and H. Xu, "Information privacy research: An interdisciplinary review," MIS Quarterly, 2011, pp. 989-1015.

[2] S. Stieger, C. Burger, M. Bohn, and M. Voracek, "Who commits virtual identity suicide? Differences in privacy concerns, internet addiction, and personality between Facebook users and quitters," Cyberpsychology, Behavior, and Social Networking, 2013, 16(9), pp. 629-634.

[3] F. Bélanger and R. E. Crossler, "Privacy in the digital age: A review of information privacy research in information systems," MIS Quarterly, 2011, pp. 1017-1041.

[4] T. Dinev, A. R. McConnell, and H. Jeff Smith, "Research commentary—informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the 'APCO' box," Information Systems Research, 26(4), 2015, pp. 639-655.

[5] Z. D. Ozdemir, H. Jeff Smith, and J. H. Benamati, "Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study," European Journal of Information Systems, 26(6), 2017, pp. 642-660.

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

[7] T. Dinev and P. Hart, "An extended privacy calculus model for e-commerce transactions," Information Systems Research, 17(1), 2006, pp. 61-80.

[8] T. Dienlin and M. J. Metzger, "An Extended Privacy Calculus Model for SNSs: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample," Journal of Computer-Mediated Communication, 21(5), 2016, pp. 368-383.

[9] D. Kim, K. Park, Y. Park, and J. H. Ahn, "Willingness to provide personal information: Perspective of privacy calculus in IoT services," Computers in Human Behavior, 92, 2019, pp.273-281.

[10] H. Li, J. Wu, Y. Gao, and Y. Shi, "Examining individuals' adoption of healthcare wearable devices: An empirical study from privacy calculus perspective," International Journal of Medical Informatics, 88, 2016, pp. 8-17.

[11] A. Acquisti et al., "Nudges for privacy and security: Understanding and assisting users' choices online," ACM Computing Surveys (CSUR), 50(3), 2017, pp. 1-41.

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

[13] I. Altman, The Environment and Social Behavior: Privacy, Personal Space, Territory, and Crowding, Brooks/Cole Publishing Company, Monterey, CA, 1975.

[14] *L. Palen and P. Dourish, “Unpacking ‘privacy’ for a networked world,” Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2003, pp. 129-136.
[15] B. Adam, Time and Social Theory, Temple University Press, Philadelphia, 1990.
[16] H. Berends and E. Antonacopoulou, “Time and organizational learning: A review and agenda for future research,” International Journal of Management Reviews, 16(4), 2014, pp. 437-453.
[17] B. Adam, “The timescapes challenge: Engagement with the invisible temporal,” In B. Adam, J. Hockey, P. Thompson, and R. Edwards (eds.), Research Lives through Time, University of Leeds, Leeds, 2008, pp. 7-12.
[18] B. Adam, “The temporal gaze: The challenge for social theory in the context of GM food,” The British Journal of Sociology, 51(1), 2000, pp. 125-142.
[19] Q. N. Huy, “Time, temporal capability, and planned change,” Academy of Management Review, 26(4), 2001, pp. 601-623.
[20] J. Webster and R. T. Watson, “Analyzing the Past to Prepare for the Future: Writing a Literature Review,” MIS Quarterly, 2002, xiii-xxiii.
[21] D. Shepherd and K. Sutcliffe, “Inductive top-down theorizing: A source of new theories of organization,” Academy of Management Review, 36(2), 2011, pp. 361-380.
[22] *J. B. Bayer, N. B. Ellison, S. Y. Schoenebeck, and E. B. Falk, “Sharing the small moments: Ephemeral social interaction on Snapchat,” Information. Communication & Society, 19(7), 2016, pp. 956-977.
[23] *L. Bauer, L. F. Cranor, S. Komanduri, M. L. Mazurek, M. K., Reiter, M. Sleeper and B. Ur, “The post anachronism: The temporal dimension of Facebook privacy,” Proceedings of the 12th ACM Workshop on Privacy in the Electronic Society, 2013, pp. 1-12.
[24] *X. Zhao, N. Salehi, S. Naranjit, S. Alwaalan, S. Voida, and D. Cosley, “The many faces of Facebook: Experiencing social media as performance, exhibition, and personal archive,” Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (CHI'13), 2013, pp. 1-10.
[25] *A. Novotny, “Signs of time: Designing social networking site profile interfaces with temporal contextual integrity,” In T. Tryfonas and I. Askoxylakis (eds.), Human Aspects of Information Security, Privacy, and Trust, Springer International Publishing, Switzerland, 2015, pp. 547-558.
[26] *R. E. Mohamed and S. Chiasson, “Online privacy and aging of digital artifacts,” In 14th Symposium on Usable Privacy and Security ({SOUPS} 2018), 2018, pp. 177-195.
[27] *B. Xu, P. Chang, C. L. Welker, N. N. Bazarova, and D. Cosley, “Automatic archiving versus default deletion: What snapchat tells us about ephemerality in design,” Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, 2016, pp. 1662-1675.
[28] *C. Castelluccia, E. De Cristofaro, A. Francillon, and M. A. Kaafar, “EphPub: Toward robust Ephemeral Publishing,” Proceedings of the 19th IEEE International Conference on Network Protocols, 2011, pp. 165-175.
[29] *O. Ayalon and E. Toch, “Retrospective privacy: Managing longitudinal privacy in online social networks,” Proceedings of the Ninth Symposium on Usable Privacy and Security, 2013, pp. 1-13.
[30] *O. Ayalon and E. Toch, “Not Even Past: Information Aging and Temporal Privacy in Online Social Networks,” Human-Computer Interaction, 32(2), 2017, pp. 73-102.
[31] *M. T. Khan, M. Hyun, C. Kanich, and B. Ur, “Forgotten but not gone: Identifying the need for longitudinal data management in cloud storage,” Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, ACM, 2018, pp. 1-12.
[32] *T. Schnitzler, M. Dürmuth, and C. Pöpper, “Towards contractual agreements for revocation of online data,” In IFIP International Conference on ICT Systems Security and Privacy Protection, Springer, Cham, 2019, pp. 374-387.
[33] *H. Wu, X. Fu, Z. Wang, and Y. Wang, “Self-destructing data method based on privacy cloud,” In International Conference on Logistics Engineering, Management and Computer Science (LEMCS 2015), Atlantis Press, 2015.
[34] *D. Barua, J. Kay, B. Kummerfeld, and C. Paris, “Theoretical foundations for user-controlled forgetting in scrutable long term user models,” Proceedings of the 23rd Australian Computer-Human Interaction Conference, Canberra, 2011, pp. 40-49.
[35] *M. Sleeper, J. Cranshaw, P. G. Kelley, B. Ur, A. Acquisti, L. F. Cranor and N. Sadeh, “‘I read my Twitter the next morning and was astonished’ A conversational perspective on Twitter regrets,” Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, 2013, pp. 3277-3286.
[36] *P. Anthonysamy, A. Rashid, and R. Chitchyan, “Privacy requirements: Present & future,” In 2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering in Society Track (ICSE-SEIS), 2017, pp. 13-22.
[37] *A. W. Boyd, “A longitudinal study of social media privacy behavior,” arXiv preprint arXiv: 1103.3174, 2011.
[38] *L. Kelly, G. Kerr, and J. Drennan, “Privacy concerns on social networking sites: A longitudinal study,” Journal of Marketing Management, 33(17-18), 2017, pp. 1465-1489.
[39] *R. Dey, Z. Jelveh, and K. Ross, “Facebook users have become much more private: A large-scale study,” In 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, 2012, pp. 346-352.
[40] *V. Chandrasekaran, T. Linden, K. Fawaz, B. Mutlu, and S. Banerjee, “BlackOut and Obfuscator: An Exploration of the Design Space for Privacy-Preserving Interventions for Voice Assistants,” arXiv preprint arXiv: 1812.00263, 2018.
[41] *N. Malkin, J. Deatrick, A. Tong, P. Wijesekera, S. Egelman, and D. Wagner, “Privacy Attitudes of Smart

Speaker Users," Proceedings on Privacy Enhancing Technologies, 2019(4), 2019, pp. 250-271.
[42] *d. boyd and E. Hargittai, "Facebook privacy settings: Who cares," First Monday, 15(8), 2010.
[43] *N. Gorm and I. Shklovski, "Sharing steps in the workplace: Changing privacy concerns over time," Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 2016, pp. 4315-4319.
[44] *B. Reynolds, J. Venkatanathan, J. Gonçalves, and V. Kostakos, "Sharing ephemeral information in online social networks: Privacy perceptions and behaviors," In IFIP Conference on Human-Computer Interaction, Springer, Berlin, Heidelberg, 2011, pp. 204-215.
[45] *A. Goldfarb and C. Tucker, "Shifts in privacy concerns," American Economic Review, 102(3), 2012, pp. 349-353.
[46] *M. Mondal, G. S. Yilmaz, N. Hirsch, M. T. Khan, M. Tang, C. Tran, … and E. Zheleva, "Moving beyond set-it-and-forget-it privacy settings on social media," Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, 2019, pp. 991-1008.
[47] *Y. Wang, G. Norcie, S. Komanduri, A. Acquisti, P. G. Leon, and L. F. Cranor, "'I regretted the minute I pressed share' A qualitative study of regrets on Facebook," Proceedings of the 7th Symposium on Usable Privacy and Security, 2011, pp. 1-16.
[48] *E. W. Ayaburi and D. N. Treku, "Effect of penitence on social media trust and privacy concerns: The case of Facebook," International Journal of Information Management, 50, 2020, pp. 171-181.
[49] *Y. Huang, B. Obada-Obieh, and K. Beznosov, "Amazon vs. My Brother: How Users of Shared Smart Speakers Perceive and Cope with Privacy Risks," Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, pp. 1-13.
[50] *G. Bansal and F. M. Zahedi, "Trust violation and repair: The information privacy perspective," Decision Support Systems, 71, 2015, pp. 62-77.
[51] *C. B. Jackson and Y. Wang, "Addressing the Privacy Paradox through Personalized Privacy Notifications," Proceedings of the ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2(2), 2018, pp. 1-25.
[52] *N. S. Good, J. Grossklags, D. K. Mulligan, and J. A. Konstan, "Noticing notice: A large-scale experiment on the timing of software license agreements," Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, ACM, 2007, pp. 607-616.
[53] *S. Gürses and J. van Hoboken, "Privacy after the Agile Turn," In J. Polonetsky, O. Tene, and E. Selinger (eds.), The Cambridge Handbook of Consumer Privacy, Cambridge University Press, Cambridge, 2018.
[54] *E. Cho, S. S. Sundar, S. Abdullah, and N. Motalebi, "Will Deleting History Make Alexa More Trustworthy? Effects of Privacy and Content Customization on User Experience of Smart Speakers," Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, pp. 1-13.
[55] *R. Mohamed, P. Chametka, and S. Chiasson, "The Influence of Decaying the Representation of Older Social Media Content on Simulated Hiring Decisions," Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems, 2020, pp. 1-19.
[56] *B. Zhang and S. S. Sundar, "Proactive vs. reactive personalization: Can customization of privacy enhance user experience," International Journal of Human-Computer Studies, 128, 2019, pp. 86-99.
[57] *F. Vitale, W. Odom, and J. McGrenere, "Keeping and discarding personal data: Exploring a design space," Proceedings of the 2019 on Designing Interactive Systems Conference, ACM, 2019, pp. 1463-1477.
[58] H. Nissenbaum, "Privacy as contextual integrity," Washington Law Review, 79, 2004, pp. 119-157.
[59] K. Borcea-Pfitzmann, A. Pfitzmann, and M. Berg, "Privacy 3.0: = data minimization + user control + contextual integrity," IT-Information Technology, 53(1), 2011, pp. 34-40.
[60] G. Amjad, M. S. Mirza, and C. Pöpper, "Forgetting with puzzles: Using cryptographic puzzles to support digital forgetting," Proceedings of the 8th ACM Conference on Data and Application Security and Privacy, ACM, 2018, pp. 342-353.
[61] S. Reimann and M. Dürmuth, "Timed revocation of user data: Long expiration times from existing infrastructure," Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society, ACM, 2012, pp. 65-74.
[62] M. J. Keith, J. S. Babb, and P. B. Lowry, "A longitudinal study of information privacy on mobile devices," In 2014 47th Hawaii International Conference on System Sciences, IEEE, 2014, pp. 3149-3158.
[63] A. Acquisti and J. Grossklags, "Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior," In 2nd Annual Workshop on Economics and Information Security-WEIS, 3, 2003, pp. 1-27.
[64] H. Xu, "The effects of self-construal and perceived control on privacy concerns," In 28th International Conference on Information Systems (ICIS 2007), Montreal, 2007.
[65] H. Lee, H. Park, and J. Kim, "Why do people share their context information on social network services? a qualitative study and an experimental study on users' behavior of balancing perceived benefit and risk," International Journal of Human-Computer Studies, 71(9), 2013, pp. 862-877.