Chapter 3
Revisiting APCO

Christoph Buck, Tamara Dinev, and Reza Ghaiumy Anaraky

Abstract Imagine that you are a product manager at a software company. When users disclose some information to your product, they can use all the great features you and your team have integrated into the software. Utilizing these features is essential for the success of your product: it makes users satisfied and encourages others to use the software as well. Furthermore, the user and usage data can be used to improve the product and help implementing new features over time. However, since your product collects users' data, you are worried about privacy-related issues. What causes users' privacy concerns, and what are the potential consequences of those concerns? The APCO (**A**ntecedents → **P**rivacy **C**oncerns → **O**utcomes) and enhanced APCO models provide a summary of the current scientific findings related to these questions and present them in a conceptual model. The APCO framework will help practitioners and scholars to bring different privacy-related aspects of a product to their attention and suggests how these aspects can interrelate. Throughout this chapter, we will consider a use case scenario of a fitness tracker application and discuss how APCO applies to this scenario.

3.1 Introduction

In 2011, *Management Information Systems Quarterly (MISQ)* published three papers reviewing literature on privacy—the articles of Li [1], Bélanger and Crossler [2], and Smith et al. [3]—which continue to be regarded as central works of the more

C. Buck (✉)
University of Bayreuth, Bayreuth, Germany
e-mail: christoph.buck@uni-bayreuth.de

T. Dinev
Florida Atlantic University, Boca Raton, FL, USA
e-mail: tdinev@fau.edu

R. G. Anaraky
Clemson University, Clemson, SC, USA
e-mail: rghaium@clemson.edu

B. P. Knijnenburg et al. (eds.), *Modern Socio-Technical Perspectives on Privacy*,
https://doi.org/10.1007/978-3-030-82786-1_3

recent Information Systems (IS)-driven privacy research. All three publications reviewed existing literature on the basis of a structured literature overview and derived comprehensive research models from it. Their common thread is the identification of privacy concerns as a proxy for measuring privacy and a central construct of current privacy research.

The often cited theoretical review of Smith et al. [3], titled "Information Privacy Research: An Interdisciplinary Review," gained a lot of attention in research and practice. The authors performed an integrated interdisciplinary review of privacy and privacy-related concepts, which included 320 research papers and 128 books [3]. By their work, they proposed a widely discussed framework for information privacy research—the APCO model—which has an intuitive appeal and can be easily understood by researchers and practitioners [4]. The APCO model presents a macro-model of privacy-related concepts and is divided into three main categories: the Antecedents (A), the Privacy Concerns (PC), and the Outcomes (O).

In this chapter, we provide a summary of the conceptualization of privacy and the integrated APCO model, one of the central macro-models in the scientific privacy discourse, as well as its more recent derivatives such as in Dinev et al. [5]. We discuss practical relevance and future opportunities in the post-APCO research landscape.

3.2 The APCO Model

As a result of an integrated interdisciplinary review of privacy and privacy-related concepts, Smith et al. [3] proposed the so-called APCO model—a framework for information privacy research—shown in Fig. 3.1.

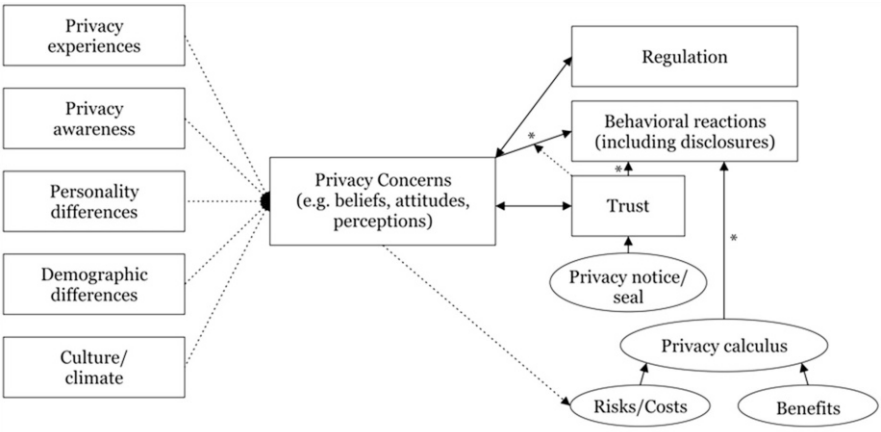

Fig. 3.1 APCO model [3]

APCO unifies information privacy literature by incorporating predominant variables used in different studies beginning with privacy concerns, the most commonly studied variable in the field. Although not as a steadfast rule [6, 7], most privacy studies suggest a negative relationship between privacy concerns and behavioral outcomes (**P**rivacy **C**oncerns → **O**utcomes). When considering the use of a fitness app, high privacy concerns can prevent users from disclosing their data or even using the application altogether. Privacy concern, itself, is shown to be a function of personal and situational cues [8]. In the APCO model, Smith et al. [3] categorize these cues as different antecedents and mark them as independent variables predicting privacy concerns (**A**ntecedents → **P**rivacy **C**oncerns). In addition, APCO also discusses trust and privacy calculus as two established predictors of privacy-behavioral outcomes.

3.2.1 The Antecedents of Privacy Concerns

Investigations of the antecedents of privacy concerns have been studied in a somewhat disjointed manner and were rarely replicated in research studies until today. The existing research today suggests that privacy concerns are influenced by the following factors:

- **Privacy experiences:** Negative privacy experiences can lead to an increase in privacy concerns [4, 9]. Thereby, if users of our fitness app had previously fallen prey to a hacker attack or a phishing attack, even if this occurred within *other* apps, they are expected to have higher levels of concern.
- **Privacy awareness:** Users' knowledge about organizational privacy practices is referred to as privacy awareness [10]. Awareness particularly increases concerns when users learn that the company used their personal data without their consent [11]. If users of our fitness tracking app know that their vital signs are being stored and sent to their physician prior to data collection, it will likely not affect their concerns [12]. However, if this data sharing initially occurs outside of their awareness, and they suddenly receive a feedback from their physician about their vital signs, this surprising revelation will likely increase their concerns.
- **Personality differences**: Various studies suggest that personality traits can affect privacy concerns. Agreeableness (being trusting, sympathetic, straightforward, and selfless) [13], for example, is shown to increase privacy concerns [14]. Other aspects of the "big five" personality traits (particularly introversion/extraversion) and independence/interdependence are also suggested to influence privacy concerns [15–17]. The privacy setting of our fitness app will likely have to be flexible enough to support a body of users that runs the gamut on these various traits.
- **Demographic differences:** Demographics are another parameter that can affect privacy concerns [18, 19]. Females and older users have higher privacy concerns than males and younger users, respectively [20, 21]. For our fitness app scenario,

we should consider gender and age in how we manage users' privacy and present privacy features to the user.
- **Culture:** Cultural values can result in different privacy concerns. For example, high masculinity cultures who prioritize material success over caring relationships (e.g., Japan) show higher concerns for unauthorized secondary usages of their personal data than low masculinity cultures (e.g., Sweden) [22]. Therefore, our fitness app may need different privacy settings or presentations in different cultures. More detailed information on cultural differences in privacy concerns and behaviors can be found in Chap. 12.

3.2.2 Privacy Concerns

Privacy concerns, the most researched construct and proxy for the investigation of privacy issues, are put at the heart of the APCO model. It acts as a dependent variable of the privacy concerns' antecedents (A) and, at the same time, as an independent variable of the privacy-related outcomes (O).

The right side of the APCO model, in which privacy concerns function as an independent variable, has so far been at the center of privacy research. First and foremost, the connection between privacy concerns and behavioral reactions was investigated in this area: a high privacy concern will lead to low levels of disclosure. However, a common drawback of this work is that it has mostly investigated behavioral intention (usually a questionnaire on willingness to disclose) rather than actual behavior (actual disclosure in a real-life scenario). According to the theory of reasoned action (TRA) [23], actual behaviors align with intentions. In the context of privacy, however, a number of researchers have demonstrated that users often disclose vast amounts of information despite their high privacy concerns [6, 24]. Privacy behaviors not being aligned to privacy concerns and intentions are referred to as privacy paradox [7]. Varian [25] describes the paradox (without naming it that way) in his work titled "Economic Aspects of Personal Privacy." According to the paradox, users articulate high privacy concerns and do not intend to purchase services that could violate their privacy (their intention) but behave in the opposite way [7, 26]. Accordingly, users show a high level of attention to data misuse, but do not change their behavior with regard to data disclosure and potential misuse. A theory-based and uniform model to explain the dichotomy described by the privacy paradox is still lacking [24]. Due to this privacy paradox, measuring the actual behavior instead of relying on a behavioral intention questionnaire seems necessary since they can be contradictory.

3.2.3 *Measuring Privacy Concerns*

Despite the omnipresence of privacy, research faces the challenge of measuring the vaguely defined, individually expressed, and subjectively perceptible construct. Privacy itself is based on insights, perceptions, and experiences and cannot always be rationalized [3]. The lack of a well-accepted and a clear definition of privacy makes the measurement of privacy difficult to operationalize.

Concerns about privacy or, shorter, privacy concerns have been an established IS research variable and are a widely recognized proxy for privacy [1, 3, 27]. Due to the broad application of privacy concerns, different perspectives and definitions of privacy concerns have developed in the scientific discourse as well. Privacy concerns can be defined as user concerns about a possible future loss of privacy as a result of voluntary or involuntary disclosure of personal data [28]. This definitional approach is followed by a broader definition of privacy per se, according to which privacy is defined as the subjective view of the users regarding fairness in the handling of personal data [10]. Many researchers use a narrower definition of privacy concerns and define them as concerns users have about the way companies and organizations handle personal information [9].

Empirical research uses mainly two constructs for privacy concerns. In the following, we discuss these two constructs as well as a third approach, which accommodates the context in measuring privacy concerns:

1. The Concern for Information Privacy (CFIP) is the first developed and verified construct for measuring informational privacy [9, 29]. This construct discusses four overall themes in privacy concern:
   (a) **Collection concerns** arise when an extensive amount of user data is being collected and stored (e.g., "It usually bothers me when companies ask me for personal information"). For our fitness app scenario, asking users for excessive amounts of information might increase collection concerns.
   (b) **Unauthorized secondary use concern** captures users' worriedness on potential unauthorized usages of their data (e.g., "Companies should never share personal information with other companies unless it has been authorized by the individual who provided the information"). For instance, users of our fitness application might willingly disclose some data to receive better trainings but at the same time might be worried about their data being shared with commercial or insurance companies.
   (c) **Improper access** reflects users' concerns about unauthorized individuals accessing their data (e.g., "Companies should devote more time and effort to preventing unauthorized access to personal information"). For example, who has the permissions to see user data in the fitness application? Is it just a machine or are there employees who can check user data too?
   (d) **Errors** capture users' concerns on accidental and deliberate errors (e.g., "companies should devote more time and effort to verifying the accuracy of the personal information in their databases"). If users of our fitness app

know that the company takes adequate precautions to minimize problems from errors, they will have less error concerns.

2. The Internet Users' Information Privacy Concerns (IUIPC) model is a further three-dimensional measurement instrument for privacy concerns, which was developed to deal more specifically with the technological conditions of the Internet [10]:

   (a) **Collection**: Similar to Smith et al. [9], collection comes first in the IUIPC dimensions.
   (b) **Control**: Users are less worried about personal data collection if they are given some degrees of control over this disclosure, e.g., if they are able to opt out [12]. If users of our fitness app are easily able to stop location tracking, and even delete the data that is already being collected, they perceive more control and thereby will have less control concerns (i.e., "Consumer online privacy is really a matter of consumers' right to exercise control and autonomy over decisions about how their information is collected, used, and shared.").
   (c) **Awareness**: Users who are not aware of how companies use their data are less likely to share information [30]. Informing users about the procedures will give them the ability to utilize *control* and choose whether they want to disclose their data or not (i.e., "It is very important to me that I am aware and knowledgeable about how my personal information will be used.").

The technological realities and the research landscape after the publication of the APCO model have offered more diverse perspectives and treatments of privacy concerns. Through this new work, privacy concerns have been studied more closely in the specific contexts. For example, the Mobile Users' Information Privacy Concerns (MUIPC) model developed constructs that account for the context and peculiarities of privacy concerns in the context of mobile systems [31]. MUIPC captures privacy concerns by secondary use of personal data, presided surveillance (similar to collection concerns discussed earlier, i.e., "I am concerned that mobile apps may monitor my activities on my mobile device."), and perceived intrusion (similar to improper access discussed earlier, i.e., "I feel that as a result of my using mobile apps, information about me is out there that, if used, will invade my privacy.").

3.2.4 Trust and Privacy Calculus

Trust is cited as one of the most important variables in the context of privacy concerns and privacy behavior. However, we believe that a clear relationship in terms of nature and direction has still not been proven. Although trust is presented as a predictor of behavioral reactions, studies also describe trust as moderator of the relationship between privacy concerns and behavioral reactions and demonstrate a

reciprocal relationship to privacy concerns. Users' trust can play an important role in our fitness tracker scenario. If we consider a direct effect of trust on behavioral reactions, increasing users' trust will result in more disclosure and in turn using more features. On the other hand, considering trust as a moderator for the effect of privacy concerns on disclosure will have different implications. In that case, trust will be less important when users have low privacy concerns. For those users with higher privacy concerns, however, trust can play an important role since a high trust can mitigate their tendencies for withholding data.

Privacy calculus is a term used to describe the privacy trade-off between the risks and the benefits of disclosure [32]. Hence, APCO considers privacy calculus as a function of perceived risks and benefits and a predictor of behavioral intention. It is worth noting that the APCO model recognizes the role of privacy calculus but treats it as a part of a more integrative process that goes on when a user decides to reveal private information. In our fitness scenario, users make a trade-off between the risk of (and maybe embarrassments resulting from) disclosing their daily intake calories and the merits of learning about the quantity of the exercise they need to undergo. This process is ongoing at least until user discloses the data or hits the next button while leaving the "daily intake calories" field empty.

The privacy calculus perspective suggests that when individuals are asked to reveal personal information to others, they deliberate on the risks involved and the potential benefits received [28]. However, this description may not paint the full picture of users' behaviors, because of bounded rationality [33]. Users may not be able to fully deliberate on risks and benefits of a disclosure decision due to cognitive limitations and a finite amount of time to make the decision. Furthermore, behavioral economics suggests that uncertainty, ambiguity, and behavioral biases also play a role in behavioral outcomes [34]. Users fall prey to nudges such as framing and default effects [35, 36]. Chapter 4 of this book will elaborate more on the behavioral economics aspect of privacy decisions.

While the influence of behavioral economic factors is evident in privacy decisions (behavioral outcome), APCO does not take such factors into account. This has prompted scholars to propose the enhanced APCO model [5], which introduces behavioral economics concepts into the APCO model.

3.3 Enhanced APCO: An Expanded View on Privacy Research

An interesting aspect of the published literature since the appearance of the APCO model can be seen in the integration of new theoretical frameworks, the incorporation of findings, effects and results from other research domains, and the application of experimental research methodologies. Already in 2015, Dinev et al. [5] reacted with a critique of the existing macro-models of privacy research and the APCO model in particular, which assume that "responses to external stimuli result

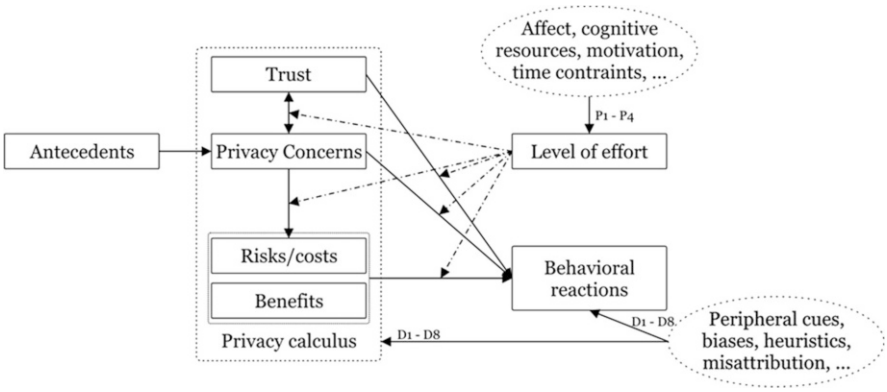

Fig. 3.2 The enhanced APCO model [5]

in deliberate analyses, which lead to fully informed privacy-related attitudes and behaviors" [5]. The scientific discourse is increasingly responding to the criticism of the assumption of complete cognitively controlled "high-effort" privacy decisions that are made under complete information [5, 25, 37], suggesting that the decisions are neither made with completely high cognitive effort nor are fully informed. Dinev et al. [5] called for an enhanced APCO model that addresses those criticisms by including concepts from behavioral economics and psychological research on cognitive processing (Fig. 3.2). In this new framework, the level of effort is specified as a moderating variable (M1) of the APCO relationships. They argue that the level of effort is influenced by factors such as affect, motivations, and temporal restrictions (P1–P4). The authors also emphasize the contextual and situational influences on privacy decisions, which have rarely been researched in IS literature but may influence the constructs of the APCO model (D1–D8). With the enhanced APCO model, Dinev et al. [5] provide a framework for further research efforts.

These ideas seemed to have caught the interests of more and more researchers. In the IS domain, for example, Adjerid et al. [38] introduce the distinction between objective and relative risks in privacy decisions, while Kehr et al. [39] examine limited cognitive resources and heuristic thinking as well as preexisting attitudes and dispositions in the situation-specific evaluation of risks and benefits in privacy decisions. Special attention in the area of "low-effort" decisions was paid to affect heuristics and the influence of affect and affective commitment [39–41]. With his study, Wakefield [42] shows that positive and negative affect has a significant effect on users' trust in websites and their privacy beliefs, which motivates the disclosure of information. Interestingly, Wakefield [42] can underline the impact intensity of affect by emphasizing that this effect is pronounced for users with high privacy concerns. Similarly, Gerlach et al. [43] investigated how users' stereotypical thinking can cause systematic judgment errors when individuals form their beliefs about an online service. In addition, they explored the effectiveness of counterstereotypic privacy statements in preventing such judgment errors [43].

Since the appearance of the APCO model and its enhanced version, numerous researchers have taken up this call for research and expanded privacy research in various directions. Due to the large contextual and situational dependence of privacy decisions, numerous approaches have been integrated into privacy research such as social cognitive theory [44], gratification theory [45], information boundary theory [45, 46], impression formation theory [47], social identity theory [48], direct causation theory and affect heuristic theory [41], and the theory of psychological ownership [49].

3.4 The Research Landscape After APCO

3.4.1 Evolution of Technology and Personalization of Services

Since the publication of the APCO model in Smith et al. [3], the importance of privacy research has continued to grow, at least due to the rapid development of digital technologies, social media, and consumer-friendly applications [4, 50]. Due to the increasing penetration of businesses in consumers' everyday life facilitated by IS, further areas of application and research have developed in many diverse contexts.

A driving factor for the increasing relevance of privacy issues is the development of mobile digital ecosystems, invisible computing, and the Internet of Things, which resulted in profound integration of IS into people's everyday life. Modern IS enable users to gain experiences that go far beyond the functional and practical applications of operationally motivated IS [51]. They can share content, experiences, knowledge, and skills as well as opportunities and even technology themselves [51]. This illustrates the changing role that products and services play in satisfying users' needs [52]. The user-centric offerings integrate the user as the co-creator of the value propositions [53]. It is the personal user data that enable these types of co-created and integrated value offerings.

The APCO model, which managed to place the individual behavior in the overall context of privacy research in an intuitive but structured way, has not lost its relevance in the scientific discourse. Although only a few authors actively classify their research work within the APCO model, its application helps to establish references to related scientific results and insights, especially in recent works.

Privacy concerns continue to serve as a central construct for measuring privacy. The majority of privacy literature includes (different forms of) privacy concerns in its considerations as a proxy for measuring privacy. Although many studies use existing and past developed measurement tools for privacy concerns, few authors began to expand or vary the spectrum of measurement instruments. Dinev et al. [54], for example, define privacy as a state and thereby establish the dependent variable perceived privacy. Other related constructs not explicitly mentioned in the APCO model include, for example, privacy self-efficacy [42] and privacy beliefs [55].

Due to the high individuality, the high contextual complexity, and the subjective perception of privacy as a personal value, it seems only sensible to strengthen the further development and adaptation of measuring instruments in the field of privacy research.

A more diverse level of analysis of APCO-related constructs and models is still desired. The majority of the studies continue to relate to the individual privacy level. Only a few studies extend this perspective to other privacy levels. Kim et al. [56], for example, point to the high level of release of group privacy based on an exploratory literature review. Although there are regulations in modern societies regarding individual privacy, this is rarely the case regarding group privacy. Societies may find a need to close this gap quickly, as, for example, social networks and virtual worlds threaten individual privacy by disregarding group privacy [56].

Two exciting and highly relevant privacy perspectives have developed in the scientific discourse in recent years: the cause and direction of privacy abuse and privacy as a serious management issue for companies. Choi et al. [57] and Teubner and Flath [58] extend the perspective of the use of personal data to the peer-to-peer (P2P) area. On P2P platforms, such as social media platforms or sharing economy platforms, personal data is no longer necessarily released or distributed by the user himself but also by other peers [4, 57]. On social media platforms, for example, friends disseminate information about users who do not necessarily want to disclose it themselves. Choi et al. [57] demonstrate in such a relationship the influence of information dissemination and network commonality on perceived privacy invasion and perceived privacy bonding.

With almost every company using personal data, privacy research is increasingly developing as a management issue for the companies. The resulting issues can be described as opportunities (exploitation) and risks (regulation, attacks). How companies deal with these challenges is the focus of a few publications, such as Greenaway et al. [59] and Oetzel and Spiekermann [60]. These works highlight the risks for companies arising from the storage of personal data and provide a tool for systematic privacy impact assessment and "privacy by design" (in European regulatory context). Privacy impact assessments (PIAs) are systematic risk assessments and scrutinize privacy implications of organizations' operations and personal data handling. The European Commission integrated PIAs into the new regulation proposal for legal data protection [61], and both European Data Protection and the US Federal Trade Commission are endorsing PIAs. Oetzel and Spiekermann [60] suggest a model for systematic step-by-step PIAs for organizations—early in the development of new products—to identify privacy risks upfront and address them accordingly. In their approach, for a new system or with a change in the system, PIA should elaborate on the characteristics of the new system, define privacy targets, and identify threats aiming those targets. Then, the PIA team should find control mechanisms to shield targets from the identified threats and document the whole process.

As already pointed by Smith et al. [3], research on the relationship between antecedents and privacy concerns (A-PC) continues to be very limited. However, Ozdemir et al. [4] demonstrate a relation between privacy awareness, privacy

experiences, and privacy concerns. Xu et al. [62], on the other hand, focus on perceived control in their work and show a relationship between the perceived control of personal information and context-specific privacy concerns. Meanwhile, Miltgen and Peyrat-Guillard [63] contributed to intercultural differences in EU countries and show that younger people feel more responsible and have more positive attitudes toward the management of personal data [63].

The post-APCO academic research continues to focus on the relationship between privacy concerns (or correlates) and outcomes (PC-O). Numerous papers focus on the interaction between trust and privacy concerns. Bansal et al. [64] show a strong correlation between privacy assurance mechanisms and trust, with privacy concerns acting as a moderating variable. In the context of location-based services, Keith et al. [44] demonstrate an effect of mobile computing self-efficacy on the confidence of users in the application as well as on the perceived risks on the disclosure of personal data. Especially in the context of mobile applications, however, classic indicators such as application quality, trust-building measures, brand recognition, and the moderating effect of privacy concerns seem to have a lower impact on the adoption of mobile services [44].

Privacy calculus and variants of costs-benefits analysis in a privacy decision continue to be a subject of intense privacy research, extending to social media. Spiekermann and Korunovska [49] provide a basic consideration of the privacy calculus through the lens of "user-centered value theory for personal data"... . Further, Karwatzki et al. [46] show that the evaluation of privacy by users is a major obstacle to the disclosure of personal data. Richey et al. [65] consider the publication of personal data and profiles via social media platforms. Interestingly, while earlier works assume a clear separation of private and professional spheres and consider the publication of private profiles as a threat to privacy, Richey et al. [65] show a contrasting effect: the respondents consciously use their private social media account to become visible to potential employers. On social network websites, Choi et al. [47] show that the expected privacy risks and social capital gains can be seen as the strongest predictors for non-acceptance or acceptance of friendship requests. For more information, please refer to Chap. 7.

The academic discussion of the personalization of IS or applications is seen through the lens of the privacy calculus in which the personalization of services usually represents an added value for the user [48]. Although the personalization of services requires the release and use of personal data, this data leads to an improved customer experience, a higher product-market fit, and an improved value proposition design. Thus, Li and Unger [66] show in the context of news and financial services that higher perceived quality and personalization can lead to an equalization of privacy concerns (see Chap. 9). Karwatzki et al. [46] and Albashrawi and Motiwalla [67], on the other hand, come to different conclusions, as they are unable to determine a significantly higher willingness to disclose data due to personalization advantages and transparency features.

3.5 Conclusion and Avenues of Future Research

Although privacy research has continued to develop positively in recent years, the APCO model has not lost its topicality in terms of structuring the research landscape. At the latest, through its extension to the enhanced APCO model, it allows both researchers and practitioners to classify questions relating to privacy decisions. The model can be used to derive references to related research work and to relate findings to one another. For example, APCO can alleviate the privacy paradox issue. To better explain privacy behaviors, rather than merely focusing on privacy concerns and risks, APCO also accounts for disclosure benefits. When disclosure results in considerable gratifications for the users, they may disclose their data even when privacy concerns are high [28, 68]. In addition, the enhanced APCO addresses the privacy paradox further by considering heuristics, since heuristics can nudge users to disclose data, regardless of their privacy concerns [26]. Overall, the IS-driven privacy research is slowly opening up to approaches from other research domains, such as psychology, behavioral economics, or marketing. There are numerous areas and opportunities for new approaches for future research work.

First and foremost, the IS research community should introduce a new term for "user." With the most recent development of ubiquitous and invisible computing, users themselves have become central actors in the digital ecosystems. They interact with IS, use networked smart everyday objects, and expand the existing system through their everyday use [69]. Since users actively contribute to value creation, they do not necessarily perceive themselves as users of a service with reference to a defined exchange relationship. For example, users of the fitness app can be content generators (e.g., by sharing success stories of reaching their goals and responding to their training experience), and their data can be used to improve the product and help others benefit from it further (e.g., to study what exercise routine results in optimal outcome for each demographic population). Therefore, the users of these IS can no longer be understood as atomistic users focused on functionality and practicability in the operational work environment. Rather, invisible computing can be explored by the users. With this new perspective, the motivation to use a system can no longer be limited to a mere fulfillment of a task but rather a contribution to the whole [51, 70]. Since invisible computing is seen as a post-desktop era in which users interact in smart environments and with smart everyday objects (Salinas Segura and Thiesse; [71]), the perspective on users should be changed [69, 72].

Building on the new user concept, future work would need to increasingly focus on the actual situation of privacy decisions and the resulting behavior. Thus, situational decisions and individual contexts represent central adjusting screws and influencing variables of human action, without which privacy decisions cannot be adequately described and researched.

Another opportunity for future research would be the focus on the antecedents of privacy and the emergence of privacy-relevant attitudes and concerns after previous work has focused predominantly on outcomes. As discussed earlier, privacy decisions are situational and contextual. Hence, it's best to measure antecedents and privacy concerns in the context.

The assumption of rising privacy concerns, inherent in numerous research projects, needs to be reexamined. The increasing use of services that pose a serious threat to the privacy of users coupled with the increasingly careless use of IS leads to the assumption that the reported growing privacy concerns are not valid. It is possible that today's complex, fully networked, and integrated IS and processes are no longer understood by the average user, who can no longer critically question or examine the ways their personal information and activity are used by various companies and stakeholders. This can raise a case for user-tailored privacy, which utilizes adaptive tools to personalize privacy to each user (Chap. 16). There may also be some sense of resignation among the users. Today, they are faced with the choice of using modern IS that intrudes their privacy or, not using it at all, with negative consequences such as technological and social exclusion.

Following the call for research by Dinev et al. [5], IS research should increasingly open up to methodological research approaches and findings from related research domains. Since digital IS are deeply and invisibly integrated into the everyday life, the social life, and social actions of groups and societies, the behavior, attitudes, and perceptions of users should be investigated in various situations that inform decision-making. Proven effects and findings from related research domains, e.g., behavioral economics, marketing, consumer behavior, or social psychology [73, 74], should be examined against the background of the digital decision-making environment, and, if necessary, new mechanisms or IS specific effects should be researched using behavioral research methods [5, 37]. As IS are user-centric and intuitive designed services, they foster low involvement and habitual buying and downloading decisions [75–77]. These environmental factors, driven by a high degree of convenience and usability, can lead to peripheral cues, heuristics and mental shortcuts, biases, and misattributions, which can affect the privacy behavior [78, 79]. Further research should consider the digital context that supports decision-making with low cognitive load. Preliminary results show a significant impact of cognitive load experiments on privacy concerns, privacy attitudes, and privacy behavior [80]. As users more and more decide, interact, and behave through the usage of complex IS, we believe that intensified research efforts in this domain will lead to progress in our understanding of privacy.

References

1. Li, Y. (2011) Empirical studies on online information privacy concerns: Literature review and an integrative framework. *CAIS* 28. https://doi.org/10.17705/1CAIS.02828
2. Bélanger, F., and R.E. Crossler. 2011. Privacy in the digital age: A review of information privacy research in information systems. *MIS Quarterly* 35: 1017–1A36.
3. Smith, H.J., T. Dinev, and H. Xu. 2011. Information privacy research: An interdisciplinary review. *MIS Quarterly* 35: 989–1015.
4. Ozdemir, Z.D., H. Jeff Smith, and J.H. Benamati. 2017. Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study. *European Journal of Information Systems* 26: 642–660. https://doi.org/10.1057/s41303-017-0056-z.

5. Dinev, T., A.R. McConnell, and H.J. Smith. 2015. Research Commentary—Informing privacy research through information systems, psychology, and behavioral economics: Thinking outside the "APCO" box. *Information Systems Research* 26: 639–655. https://doi.org/10.1287/isre.2015.0600.
6. Barnes, S.B. 2006. A privacy paradox: Social networking in the United States. *First Monday.*
7. Norberg, P.A., D.R. Horne, and D.A. Horne. 2007. The privacy paradox: Personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs* 41: 100–126.
8. Xu, H., T. Dinev, H.J. Smith, and P. Hart. 2008. Examining the formation of individual's privacy concerns: Toward an integrative view. In *ICIS 2008 Proceedings*.
9. Smith, H.J., S.J. Milberg, and S.J. Burke. 1996. Information privacy: Measuring individuals' concerns about organizational practices. *MIS Quarterly* 20: 167. https://doi.org/10.2307/249477.
10. Malhotra, N.K., S.S. Kim, and J. Agarwal. 2004. Internet Users' Information Privacy Concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research* 15: 336–355. https://doi.org/10.1287/isre.1040.0032.
11. Cespedes, F.V., and H. Jeff Smith. 1993. Database marketing: New rules for policy and practice. *Sloan Management Review* 34. https://www.proquest.com/openview/8ce0a3e960946f7a684c13badd19eb89/1?pq-origsite=gscholar&cbl=26142.
12. Nowak, G.J., and J. Phelps. 1995. Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing* 9 (3): 46–60. https://doi.org/10.1002/dir.4000090307.
13. Terracciano, A., R.R. McCrae, D. Hagemann, and P.T. Costa Jr. 2003. Individual difference variables, affective differentiation, and the structures of affect. *Journal of Personality* 71 (5): 669–704. https://doi.org/10.1111/1467-6494.7105001.
14. Korzaan, M.L., and K.T. Boswell. 2008. The influence of personality traits and information privacy concerns on behavioral intentions. *Journal of Computer Information Systems* 48 (4): 15–24. https://doi.org/10.1080/08874417.2008.11646031.
15. Xu, H. 2007. The effects of self-construal and perceived control on privacy concerns. In *ICIS 2007 Proceedings*, 125. http://aisel.aisnet.org/icis2007/125.
16. Bansal, G., and D. Gefen. 2015. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems* 24 (6): 624–644. https://doi.org/10.1057/ejis.2014.41.
17. Lu, Y., B. Tan, and K.-L. Hui. 2004. Inducing customers to disclose personal information to internet businesses with social adjustment benefits. In *ICIS 2004 Proceedings*, 45. https://aisel.aisnet.org/icis2004/45.
18. Culnan, M.J., and P.K. Armstrong. 1999. Information privacy concerns, procedural fairness, and impersonal trust: An empirical investigation. *Organization Science* 10: 104–115. https://doi.org/10.1287/orsc.10.1.104.
19. Chen, K., and A.I. Rea Jr. 2004. Protecting personal information online: A survey of user privacy concerns and control techniques. *Journal of Computer Information Systems* 44 (4): 85–92. https://doi.org/10.1080/08874417.2004.11647599.
20. Youn, S., and K. Hall. 2008. Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *Cyberpsychology and Behavior* 11 (6): 763–765. https://doi.org/10.1089/cpb.2007.0240.
21. Hoy, M.G., and G. Milne. 2010. Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising* 10 (2): 28–45. https://doi.org/10.1080/15252019.2010.10722168.
22. Bellman, S., E.J. Johnson, S.J. Kobrin, and G.L. Lohse. 2004. International differences in information privacy concerns: A global survey of consumers. *The Information Society* 20 (5): 313–324. https://doi.org/10.1080/01972240490507956.
23. Fishbein, M, and I. Ajzen. 1975. *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research*.

24. Kokolakis, S. 2017. Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon. *Computers & Security* 64: 122–134. https://doi.org/10.1016/j.cose.2015.07.002.
25. Varian, H.R. 2009. Economic aspects of personal privacy. In *Internet Policy and Economics*, ed. L.M. Pupillo and W.H. Lehr, 2nd ed., 101–109. Dordrecht: Springer.
26. Acquisti, A., and J. Grossklags. 2005. Privacy and rationality in individual decision making. *IEEE Security & Privacy Magazine* 3: 26–33. https://doi.org/10.1109/MSP.2005.22.
27. Hong, W., and J.Y.L. Thong. 2013. Internet privacy concerns: An integrated conceptualization and four empirical studies. *MIS Quarterly* 37: 275–298.
28. Dinev, T., and P. Hart. 2006. An extended privacy calculus model for e-commerce transactions. *Information systems research* 17: 61–80. https://doi.org/10.1287/isre.1060.0080.
29. Stewart, K.A., and A.H. Segars. 2002. An empirical examination of the concern for information privacy instrument. *Information systems research* 13: 36–49. https://doi.org/10.1287/isre.13.1.36.97.
30. Hoffman, D.L., T.P. Novak, and M. Peralta. 1999. Building consumer trust online. *Communications of the ACM* 42 (4): 80–85. https://doi.org/10.1145/299157.299175.
31. Xu, H., S. Gupta, M. Rosson, and J. Carroll. 2012. Measuring mobile users' concerns for information privacy. In *ICIS 2012 Proceedings*.
32. Laufer, R.S., and M. Wolfe. 1977. Privacy as a concept and a social issue: A multidimensional developmental theory. *Journal of Social Issues* 33: 22–42. https://doi.org/10.1111/j.1540-4560.1977.tb01880.x.
33. Simon, H.A. 1955. A behavioral model of rational choice. *The Quarterly Journal of Economics* 69 (1): 99–118. https://doi.org/10.2307/1884852.
34. Grossklags, J., and A. Acquisti. 2007. When 25 cents is too much: An experiment on willingness-to-sell and willingness-to-protect personal information. In *WEIS*. https://econinfosec.org/archive/weis2007/papers/66.pdf.
35. Johnson, E.J., S. Bellman, and G.L. Lohse. 2002. Defaults, framing and privacy: Why opting in-opting out 1. *Marketing Letters* 13 (1): 5–15. https://doi.org/10.1023/A:1015044207315.
36. Bahirat, P., Q. Sun, and B.P. Knijnenburg. 2018. Scenario context V/s framing and defaults in managing privacy in household IoT. In *Proceedings of the 23rd International Conference on Intelligent User Interfaces Companion*, 1–2.
37. Goes, P.B. 2013. Editor's Comments: Information systems research and behavioral economics. *MIS Quarterly* 37: iii–viii.
38. Adjerid, I., E. Peer, A. Acquisti. 2016. *Beyond the Privacy Paradox: Objective Versus Relative Risk in Privacy Decision Making*.
39. Kehr, F., T. Kowatsch, D. Wentzel, and E. Fleisch. 2015. Blissfully ignorant: The effects of general privacy concerns, general institutional trust, and affect in the privacy calculus. *Information Systems Journal* 25: 607–635. https://doi.org/10.1111/isj.12062.
40. Kordzadeh, N., and J. Warren. 2014. Communicating personal health information in virtual health communities: A theoretical framework. In *IEEE 8th International Symposium on Service-Oriented System Engineering (SOSE), Oxford, United Kingdom, 7–11 April 2014 [including workshop/symposium papers]*, 636–645. Piscataway, NJ: IEEE.
41. Yu, J., P.J.-H. Hu, and T.-H. Cheng. 2015. Role of affect in self-disclosure on social network websites: A test of two competing models. *Journal of Management Information Systems* 32: 239–277. https://doi.org/10.1080/07421222.2015.1063305.
42. Wakefield, R. 2013. The influence of user affect in online information disclosure. *The Journal of Strategic Information Systems* 22: 157–174. https://doi.org/10.1016/j.jsis.2013.01.003.
43. Gerlach, J., P. Buxmann, and T. Dinev. 2018. 'They're All the Same!' Stereotypical thinking and systematic errors in users' privacy-related judgments about online services. *Journal of the Association for Information Systems* 19: 247–265.
44. Keith, M.J., J.S. Babb, P.B. Lowry, C.P. Furner, and A. Abdullat. 2015. The role of mobile-computing self-efficacy in consumer information disclosure. *Information Systems Journal* 25: 637–667. https://doi.org/10.1111/isj.12082.

45. Sutanto, J., E. Palme, C.-H. Tan, and C.W. Phang. 2013. Addressing the personalization-privacy paradox: An empirical assessment from a field experiment on smartphone users. *MIS Quarterly* 37: 1141–1164.
46. Karwatzki, S., O. Dytynko, M. Trenz, and D. Veit. 2017. Beyond the personalization–privacy paradox: Privacy valuation, transparency features, and service personalization. *Journal of Management Information Systems* 34: 369–400. https://doi.org/10.1080/07421222.2017.1334467.
47. Choi, B., Y. Wu, J. Yu, and L. Land. 2018. *Love at First Sight: The Interplay Between Privacy Dispositions and Privacy Calculus in Online Social Connectivity Management*. 1536–9323
48. Shih, H.-P., K.-h. Lai, and T.C.E. Cheng. 2017. Constraint-based and dedication-based mechanisms for encouraging online self-disclosure: Is personalization the only thing that matters? *European Journal of Information Systems* 26: 432–450. https://doi.org/10.1057/s41303-016-0031-0.
49. Spiekermann, S., and J. Korunovska. 2017. Towards a value theory for personal data. *Journal of Information Technology* 32: 62–84. https://doi.org/10.1057/jit.2016.4.
50. Lowry, P.B., T. Dinev, and R. Willison. 2017. Why security and privacy research lies at the centre of the information systems (IS) artefact: Proposing a bold research agenda. *European Journal of Information Systems* 26: 546–563. https://doi.org/10.1057/s41303-017-0066-x.
51. Sullivan, J., R. Scheepers, and C. Middleton. 2009. Conceptualizing user satisfaction in the ubiquitous computing era. In *ICIS 2009 Proceedings*.
52. Merli, G. 2013. The transformation of the business model: Business modelling. In *New Business Models and Value Creation: A Service Science Perspective*, ed. L. Cinquini, A. Di Minin, and R. Varaldo, 67–86. Milan: Springer.
53. Vargo, S.L., and R.F. Lusch. 2008. Service-dominant logic: Continuing the evolution. *Journal of the Academy of Marketing Science* 36: 1–10. https://doi.org/10.1007/s11747-007-0069-6.
54. Dinev, T., H. Xu, J.H. Smith, and P. Hart. 2013. Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems* 22: 295–316. https://doi.org/10.1057/ejis.2012.23.
55. Gerlach, J., T. Widjaja, and P. Buxmann. 2015. Handle with care: How online social network providers' privacy policies impact users' information sharing behavior. *The Journal of Strategic Information Systems* 24: 33–43. https://doi.org/10.1016/j.jsis.2014.09.001.
56. Kim, J., R.L. Baskerville, and Y. Ding. 2018. Breaking the privacy kill chain: Protecting individual and group privacy online. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-018-9856-5.
57. Choi, B.C.F., Z. Jiang, B. Xiao, and S.S. Kim. 2015. Embarrassing exposures in online social networks: An integrated perspective of privacy invasion and relationship bonding. *Information Systems Research* 26: 675–694. https://doi.org/10.1287/isre.2015.0602.
58. Teubner, T., and C. Flath. 2019. Privacy in the sharing economy. *Journal of the Association for Information Systems* 20. https://doi.org/10.17705/1jais.00534.
59. Greenaway, K.E., Y.E. Chan, and R.E. Crossler. 2015. Company information privacy orientation: A conceptual framework. *Information Systems Journal* 25: 579–606. https://doi.org/10.1111/isj.12080.
60. Oetzel, M.C., and S. Spiekermann. 2014. A systematic methodology for privacy impact assessments: A design science approach. *European Journal of Information Systems* 23: 126–150. https://doi.org/10.1057/ejis.2013.18.
61. Gutwirth, S., R. Leenes, P. De Hert, and (Eds.). 2015. *Reforming European Data Protection Law*. Vol. 20. Dordrecht: Springer. https://doi.org/10.1016/B978-0-12-802122-4.00002-X.
62. Xu, H., H.-H. Teo, B.C.Y. Tan, and R. Agarwal. 2012b. Research Note —Effects of individual self-protection, industry self-regulation, and government regulation on privacy concerns: A study of location-based services. *Information Systems Research* 23: 1342–1363. https://doi.org/10.1287/isre.1120.0416.
63. Miltgen, C.L., and D. Peyrat-Guillard. 2014. Cultural and generational influences on privacy concerns: A qualitative study in seven European countries. *European Journal of Information Systems* 23: 103–125. https://doi.org/10.1057/ejis.2013.17.

64. Bansal, G., F.M. Zahedi, and D. Gefen. 2015. The role of privacy assurance mechanisms in building trust and the moderating role of privacy concern. *European Journal of Information Systems* 24: 624–644. https://doi.org/10.1057/ejis.2014.41.
65. Richey, M., A. Gonibeed, and M.N. Ravishankar. 2018. The perils and promises of self-disclosure on social media. *Information Systems Frontiers* 20: 425–437. https://doi.org/10.1007/s10796-017-9806-7.
66. Li, T., and T. Unger. 2012. Willing to pay for quality personalization? Trade-off between quality and privacy. *European Journal of Information Systems* 21: 621–642. https://doi.org/10.1057/ejis.2012.13.
67. Albashrawi, M., and L. Motiwalla. 2017. Privacy and personalization in continued usage intention of mobile banking: An integrative perspective. *Information Systems Frontiers.* https://doi.org/10.1007/s10796-017-9814-7.
68. Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication*, 83–108.
69. Yoo. 2010. Computing in everyday life: A call for research on experiential computing. *MIS Quarterly* 34: 213. https://doi.org/10.2307/20721425.
70. Borriello, G. 2008. Invisible computing: Automatically using the many bits of data we create. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 366: 3669–3683. https://doi.org/10.1098/rsta.2008.0128.
71. Zhao, R., and J. Wang. 2011. Visualizing the research on pervasive and ubiquitous computing. *Scientometrics* 86: 593–612. https://doi.org/10.1007/s11192-010-0283-8.
72. Lamb, R., and R. Kling. 2003. Reconceptualizing users as social actors in information systems research. *MIS Quarterly* 27: 197. https://doi.org/10.2307/30036529.
73. Acquisti, A., L. Brandimarte, and G. Loewenstein. 2015. Privacy and human behavior in the age of information. *Science* 347: 509–514. https://doi.org/10.1126/science.aaa1465.
74. Ariely, D. 2009. The end of rational econonmics. *Harvard Business Review* 87: 78–84.
75. Aarts, H., and A.P. Dijksterhuis. 2000. The automatic activation of goal-directed behaviour: The case of travel habit. *Journal of Environmental Psychology* 20: 75–82.
76. Buck, C., C. Horbel, T. Kessler, and C. Christian. 2014. Mobile consumer apps: Big data brother is watching you. *Marketing Review St. Gallen* 31: 26–35. https://doi.org/10.1365/s11621-014-0318-2.
77. Dijksterhuis, A., P.K. Smith, R.B. van Baaren, and D.H.J. Wigboldus. 2005. The unconscious consumer: Effects of environment on consumer behavior. *Journal of Consumer Psychology* 15: 193–202. https://doi.org/10.1207/s15327663jcp1503_3.
78. Anaraky, R., B.P. Knijnenburg, and M. Risius. 2020. Exacerbating mindless compliance: The danger of justifications during privacy decision making in the context of Facebook applications. *AIS Transactions on Human-Computer Interaction*: 70–95.
79. Buck, C., S. Burster, and T. Eymann. 2018. An experiment series on app information privacy concerns. In *26th European Conference on Information Systems (ECIS)*.
80. Buck, C., and T. Dinev. 2019. Verifying effects and findings of behavioral economics and social psychology in information systems and digital decision-making environments using experimental research approaches. *Research in Progress*.