Assessing Theories for Research on Personal Data Transparency

Anette Siebenkäs, Dirk Stelzer

Assessing Theories for Research on Personal Data Transparency

Anette Siebenkäs[0000-0002-0123-4795] and Dirk Stelzer[0000-0002-6757-9411]

Technische Universität Ilmenau, Germany,
Fachgebiet Informations- und Wissensmanagement
Postfach 10 05 65, D-98693 Ilmenau
anette.siebenkaes@tu-ilmenau.de, dirk.stelzer@tu-ilmenau.de

Abstract. A growing number of business models are based on the collection, processing and dissemination of personal data. For a free decision about the disclosure of personal data, the individual concerned needs transparency as insight into which personal data is collected, processed, passed on to third parties, for what purposes and for what time (Personal Data Transparency, or PDT for short). The intention of this paper is to assess theories for research on PDT. We performed a literature review and explored theories used in research on PDT. We assessed the selected theories that may be appropriate for exploring PDT. Such research may build on several theories that open up different perspectives and enable various fields of study.

Keywords: Personal Data Transparency, Literature Review, Theory, Information Privacy, Ex-ante transparency, Real-time transparency, Ex-post transparency.

1 Introduction

An increasing number of business models are based on the collection, processing and dissemination of personal data [16, 39, 48, 65].

Personal data is defined as "any information relating to an identified or identifiable natural person" [46]. Personal data may be used for purposes that could harm the data subject. This threatens the right to informational self-determination [37]. For a free decision about disclosing personal data, the individual concerned needs transparency.

Transparency requires insight into which personal data is collected, processed, passed on to third parties, for what purposes and for what time. We call transparency of personal data processing Personal Data Transparency (or PDT for short). PDT is a privacy principle and a prerequisite for informational self-determination [22, 46].

Although PDT is demanded by legislators, consumer protection associations, privacy commissioners and data protection officers to ensure consumers' privacy [46] and consumers explicitly ask for transparency [31], findings from several research projects suggest that enhanced transparency may overstrain consumers [26, 40, 59, 62] and decrease users' privacy concerns and risk beliefs [2, 8, 14, 45, 47]. Therefore, enhanced

PDT – originally meant as a means of increasing consumer protection – may indeed lead to less privacy.

Theories provide a lens for issues and challenges worthy of scientific research. They also help to pose interesting research questions and guide the selection of research methods. Theories are practical because they help to accumulate knowledge and to integrate findings of different scholars and research projects in a systematic manner [21]. Our research may support scholars in identifying, assessing, selecting or adapting theories when exploring PDT.

Research into PDT is a subset of information privacy research. When starting our research, we were working on the assumption that many scholars who explore PDT apply theories that are also used in other areas of information privacy research.

The intention of this paper is to assess theories for research on PDT. In particular, we address the following research questions:

RQ1: Are there theories that can substantially support research in the field of PDT?

RQ2: What are strengths and weaknesses of theories used to investigate PDT?

We followed a two-step approach. First, we performed a literature review to analyse which theories scholars use when investigating PDT. We based our review on Rowe's [49] recommendations for conducting literature reviews. To distinguish conceptual foundations from theories, we drew on Sutton, Staw and Gregor [21, 55]. Then, we defined criteria that a theory appropriate for exploring PDT should cover. We used these criteria for assessing the selected theories.

2 Theories Used in PDT-Research

2.1 Literature Review

For identifying theories appropriate for exploring PDT, we focused on papers published between 2000 and 2017 and queried the following databases: ACM Digital Library, AIS Electronic Library, EBSCO, Elsevier ScienceDirect, IEEE Xplore Digital Library, INFORMS PubsOnline, SpringerLink and Web of Science.

We searched titles, abstracts and keywords with the following search term: *(transparent OR transparency) AND (privacy OR personal data OR personal information)*. Our focus was on journal articles, conference proceedings and book chapters written in English. By reading article titles, abstracts and introductions, we identified and selected papers for further review. We conducted backward and forward searches, following Webster and Watson [64]. We identified 157 papers relevant to PDT. Within these articles, we searched for "theor*" in the full texts of the papers which led to 42 papers for in-depth review. We read relevant passages, in particular theoretical and conceptual foundations. Subsequently, we identified and analysed the original sources of the theories quoted in the papers. Theories quoted in only one of the 42 papers or theories that refer to contexts not directly relevant for the purpose of our research (such as the Theory of Cryptography) were excluded. We included 21 papers in the final selection. Several authors base their research not only on one theory, but combine different theories into a new research construct. Papers that we considered relevant in this context, were assigned to the theory that was predominantly used in the respective papers.

Table 1 gives an overview of theories identified in our study, the original sources and the papers that apply – or at least quote – these theories (Table 1).

Table 1. Theories Used in Research on PDT

Theories	Sources explaining the theories	Sources applying the theories
Agency Theory Signaling Theory	Eisenhardt [15], Spence [53]	Greenaway et al. [19], Monteleone [36], Pollach [44]
Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB)	Ajzen and Fishbein [4], Ajzen and Fishbein [3]	Awad and Krishnan [6], Cabinakova et al. [9], Kowatsch and Maass [31]
Technology Acceptance Model (TAM)	Davis [11]	Cabinakova et al. [9], Kowatsch and Maass [31], Zhang and Xu [66]
Theory of Bounded Rationality	Simon [51, 52]	Acquisti et al. [1], Adjerid et al. [2], Brandimarte et al. [8], Monteleone [36], Zhang and Xu [66]
Prospect Theory	Tversky and Kahneman [60, 61], Kahneman and Tversky [29]	Acquisti et al. [1], Adjerid et al. [2], Monteleone [36], Walker [62]
Information Boundary Theory (IBT), Communication Privacy Management Theory (CMPT)	Altmann [5] Petronio [42, 43]	Dinev et al. [14], Hauff et al. [24], Karwatzki et al. [30], Rader [47], Stutzman et al. [54]
Restricted Access/Limited Control Theory of Privacy (RALC)	Tavani and Moor [58], Tavani [56, 57]	Brandimarte et al. [8], Pardo and Siemens [41]
Theory of Contextual Integrity	Nissenbaum [38–40], Barth et al. [7]	Hildén [27], Ifenthaler and Schumacher [28], Tene and Polenetsky [59]
Procedural Fairness Theory / Procedural Justice (adapted to privacy)	Greenberg [20], Lind and Tyler [34], Culnan and Armstrong [10]	Cabinakova et al. [9], Dinev et al. [12, 14], Greenaway et al. [19], Hauff et al. [24], Karwatzki et al. [30], Pollach [44]
Social Contract Theory (adapted to privacy) Privacy Calculus, Extended Privacy Calculus Dual Calculus	Milne and Gordon [35], Laufer and Wolfe [32], Culnan and Armstrong [10], Dinev and Hart [13], Li [33]	Awad and Krishnan [6], Cabinakova et al. [9], Dinev et al. [12, 14], Greenaway et al. [19], Kowatsch and Maass [31]
Utility-maximization Theory (adapted to privacy)	Rust [50]	Awad and Krishnan [6], Kowatsch and Maass [31]

2.2 Assessing Theories

In our literature review, we identified authors referring to established theories and concepts from other disciplines such as psychology, sociology and economics. Other authors, mostly engaged in design research, refer to concepts from information systems

and computer science. Several authors draw on privacy theories. In the selected papers mentioned in table 1, authors exploring PDT either use general theories or privacy theories or general theories that have been contextualized and adapted to the privacy sphere. We call a theory a general theory when it is highly abstract and separate from specific application areas. Privacy theories are theories that were developed solely for exploring privacy. None of the authors identified in our literature review has developed a specific theory for PDT or has drawn on a native PDT theory.

We use the following questions to assess the theories:

1. Does the theory address information privacy?
2. Have scholars adapted the theory for privacy research?
3. Does the theory cover aspects that may be relevant for the study of PDT?
4. Which aspects of PDT are or can be considered when using the theory?

Table 2 provides answers to questions 1 to 3.

Table 2. Assessment of Theories (Questions 1 to 3)

Theory	1. Information Privacy Theory?	2. Adaption to Privacy Research?	3. Aspects of PDT considered?
Agency Theory Signaling Theory	no	yes [19]	yes
Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB)	no	partly used for studying privacy decision-making	yes
Technology Acceptance Model	no	yes, adapted in [9, 31, 66]	yes [9, 31]
Theory of Bounded Rationality	no	partly used for studying privacy decision-making	no
Prospect Theory	no	partly used for studying privacy decision-making	no
Information Boundary Theory (IBT), Communication Privacy Management Theory (CMPT)	yes	-	yes [24, 30, 47, 54]
Restricted Access /Limited Control Theory of Privacy (RALC)	yes	-	no
Theory of Contextual Integrity	yes	-	yes
Procedural Fairness Theory / Procedural Justice (adapted to privacy)	yes	-	yes [19]
Social Contract Theory (adapted to privacy), Privacy Calculus, Extended Privacy Calculus, Dual Calculus	yes	-	yes [6, 14]
Utility-maximization Theory (adapted to privacy)	yes	-	yes [6, 14]

For answering question 4, we draw on the following characterization of transparency:

> *"Transparency aims at an adequate level of clarity of the processes in privacy-relevant data processing so that the collection, processing and use of the information can be understood and reconstructed at any time. Further, it is important that all parties involved can comprehend the legal, technical, and organizational conditions setting the scope for this processing. This information has to be available before, during and after the processing takes place. Thus, transparency has to cover not only the actual processing, but also the planned processing (ex-ante transparency) and the time after the processing has taken place to know what exactly happened (ex-post transparency)."* [23]

Based on this characterization, a theory for describing, analysing, explaining or predicting PDT should address at least one of the following questions:

(a) Does the theory address supply of ***information about collection, processing, use or dissemination of personal data***?
(b) Which ***parties involved*** in processing personal data does the theory address?
(c) Is the focus of the theory on the ***process of providing information*** or on ***individual traits of data subjects*** (e.g. intention, decision-making or behaviour)?
(d) Does the theory deal with ***the point in time*** at which information is made available?

We regard the data subject as the producer and owner of the personal data on the one hand and the data controller as the representative for all parties involved in the collection, processing, use and distribution on the other hand. In this context, the data subject is "an identified or identifiable natural person" [46], whose personal data is provided to a data controller as a "natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data" [46]. Other parties involved can be the data processor that processes the personal data on behalf of the controller, recipients of the personal data and third parties. Transparency-enhancing information about data protection measures taken by the controller is also relevant for supervising authorities and consumer protection associations. We have shown this in Figure 1. In the following text however, we focus on data subjects and data controllers and abstract from supervisory authorities.

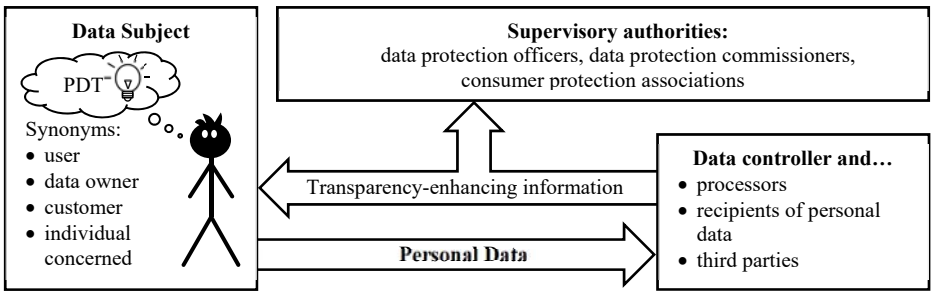

Fig. 1. Parties involved

In the following sections, we discuss which aspects of PDT are considered by the selected theories. A brief characterization of the theories is included. Core concepts are marked in italics. The characters in brackets refer to the questions (a) to (d) mentioned above.

Agency Theory, Information Asymmetry and Signaling Theory

Agency Theory describes *principal-agent relationships* in transactions with *information asymmetries* [15]. **Signaling Theory** addresses options to reduce information asymmetry by *screening* (the principal monitors the agent) or *signaling* (the agent provides information to the principal) [53].

Agency Theory, Information Asymmetry and Signaling Theory are economic theories. These theories can be applied in the data protection / privacy context. Greenaway et al. [19] developed a "Company information privacy orientation framework" based on several theories, including Agency Theory. A lack of PDT for a user as the principal can be considered as an information asymmetry. In this case, screening (e.g. the user as the data subject monitors the company as the data controller with a transparency-enhancing tool) or signaling (the data controller provides information for understanding collection, processing and use of personal data) are opportunities to reduce information asymmetries (a). The parties involved are the data subject as the principal and the data controller as the agent (b). The focus of Agency Theory is on information asymmetry and exchange and not on individual traits of principal or agent. The relationship between principal and agent and the exchange of transparency-enhancing information can be investigated (c). The time of information availability is irrelevant in this context (d).

Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), Reasoned Action Approach (RAA)

The **TRA** by Ajzen and Fishbein [4] and the **TPB** by Ajzen and Fishbein [3] are two classical behavioural theories from psychology. They aim to explore the effect of *attitudes* and *subjective norms* on *behaviour intention* and *behaviour*. TPB also considers *perceived behaviour control*. In 2010, Fishbein and Ajzen released a joint theory named the **Reasoned Action Approach** which aims at "predicting and changing social behaviour" [17]. This approach extends TRA and TPB. *Attitude, perceived norm and perceived behaviour control* are influenced by the individual beliefs (*behavioural beliefs, normative beliefs and control beliefs).* These beliefs are based on *background factors*: *individual factors* (e.g. personality and past behaviour), *social factors* (e.g. education, age, gender, culture) and *information factors* (knowledge, media, intervention). Intention and behaviour are moderated by *actual control* (skills, abilities, environment). These theories are an important basis for the development of further, adapted theories, e.g. the Technology Acceptance Model.

TRA, TPB and RAA are general theories focussing on human behaviour and not on PDT. Several papers included in our review use one of these theories or elements thereof [6, 9, 31]. In RAA, actual control moderates individual intention and behaviour. With a theory based on RAA, disclosing personal data can be studied by specifying

actual control with transparency-enhancing measures. These measures provide information about collection, processing, use or dissemination of personal data (a). The focus is on the data subject (b) and her/his data disclosure behaviour (c). For actual control, the time when transparency-enhancing measures are available is of particular interest as only information provided before or during disclosure of personal data enables a well-informed decision about disclosing, i.e. actual control (d).

Technology Acceptance Model (TAM)

The **Technology Acceptance Model (TAM)** was developed on the basis of TRA by Davis [11] as an instrument for evaluating the acceptance of information technologies. Users' *perceived usefulness* and *perceived ease of use* determine *behavioural intention to use* and *actual system use*.

TAM was not specifically designed for exploring privacy, but it was adapted for evaluating acceptance of transparency-enhancing tools, e.g. in [9, 31, 66]. Cabinakova et al. [9] base their empirical analysis on TAM, TPB and the Privacy Calculus. They studied how *information about personal data processing* presented by the Google dashboard influences trust in the dashboard and in the dashboard provider, Google (a). Data subject (service user) and data controller (dashboard provider) are addressed by the theory (b). The focus lies on individual behaviour intention (c). The time of information availability is not taken into account (d). Kowatsch and Maass [31] draw on TAM, Utility-maximization Theory and Extended Privacy Calculus for exploring usage intentions and individuals' willingness to provide personal information to Internet of Things services. Survey participants were asked about their expectations on being informed about personal data usage (a). The focus lies on the opinion of potential users of the Internet of Things services (b). The authors studied participants' expectations but they did not explore how transparency affects planned usage of Internet of Things services (c). Participants were asked whether they prefer to be informed every time personal data is used or only the first time (d).

Theory of Bounded Rationality

Unlike Agency Theory, TRA, TPB and RAA, which consider human decisions to be rational, the **Theory of Bounded Rationality** assumes *limited rationality*. *Cognitive limitations, time constraints* and *environmental factors* influence human decisions. Instead of striving to achieve an optimum, individuals try to reach satisfactory levels. The individual uses *heuristics* in decision-making to deal with a complex situation [51].

In the privacy context, the Theory of Bounded Rationality has been used to describe the issue of people not understanding the consequences of personal data disclosure [8, 66] and of information overload as potential inhibitor of disclosing personal data [36]. The theory does not address supply of information about collection, processing, use or dissemination of personal data (a). The focus lies on individual traits of data subjects, i.e. decision-making behaviour (b, c). As the time when information is made available may affect decision-making, this theory is appropriate for describing how and when PDT should be provided in the context of bounded rationality (d).

Prospect Theory

Another behavioural aspect in decision-making is considered in **Prospect Theory**. Prospect Theory explores *decision-making under risk* when an individual selects from *probabilistic alternatives*. The *losses and gains* of this process seem to be more important than the final outcome, leading to a *risk-avoiding behaviour* [29, 60, 61].

Prospect Theory in privacy research can be used to explore the decision-making process of individuals who consider disclosing personal data. PDT, however is not in the focus of the theory (a). In studies of privacy behaviour based on Prospect Theory, "biases in judgements" [60] and the heuristics that data subjects use for decision-making are of interest (b, c). The theory does not explicitly deal with the time when information is made available for transparency reasons (d).

Information Boundary Theory (IBT), Communication Privacy Management Theory (CMPT)

Theoretical contributions to privacy date back to Warren and Brandeis [63] stressing the "right to be left alone". In the **Information Boundary Theory (IBT,** also called Privacy Regulation Theory), Altman [5] discusses *privacy as a dynamic process of boundary regulation* and a "selective control of access to the self or to one's group". Altman states five properties of IBT: *Temporal dynamic process of interpersonal boundary, desired and actual levels of privacy, non-monotonic function of privacy, bi-directional nature of privacy, two levels of privacy (individual and group privacy)* [5].

Petronio [43] integrated these concepts into the **CPMT** and shifted Altman's theory into virtual space. *Private boundaries* separate private and public information. Sharing private information leads to a *collective boundary*, including the individual and the group with which the information was shared. For the individual, it is important to know the communication context for deciding about personal data disclosure. She or he creates a set of rules for the disclosure decision, for example 'I always share my party pictures with my friends, but not with my employer'. The rules are based on five criteria: two *core criteria (cultural and gender)* and *three catalyst criteria (context, motivation, and risk/benefit ratio)* [43].

Applying IBT, Hauff et al. [24] investigate the disposition to value privacy in the context of personalized services. According to IBT, situational factors moderate a person's privacy concerns and risk assessment. "Situation factors represent the degree of personalization and transparency offered to a customer." [24]. The theory does not specifically address supply of transparency-enhancing information. However, the degree of PDT may influence individual information boundaries (a). Hauff et al. [24] explore disclosure behaviour of data subjects (b) as a function of enhanced or reduced PDT in service personalisation (c). The time of providing information to service users is not explicitly considered (d). Other examples of applying components of IBT and CMPT are described by Karwatzki et al. [30], Rader [47] and Stutzmann et al. [54].

Recently proposed privacy theories are more involved with the idea of data protection. The RALC Theory by Tavani and Moor [46] and Nissenbaum's Theory of Contextual Integrity [38–40] are two of them [25].

Restricted Access/Limited Control Theory of Privacy (RALC)

The Restricted Access/Limited Control Theory of Privacy (RALC) by Tavani and Moor [58] seeks to join *limitation* and *control* as two concepts of former privacy theories and to lay a foundation for further privacy theories [25, 58]. Tavani [56, 57] distinguishes between restricted access theories, control theories and restricted access/limited control theories (RALC) of privacy [18]. In the first set of theories, privacy is ensured by *restricting access to personal data*. Control theories place greater emphasis on the individual. They perceive *privacy as control and self-determination of data subjects over information about themselves*. The RALC theory combines both approaches. *Restricted access* refers to a sphere that protects individuals from privacy intrusions. *Limited control* refers to management of privacy that enables consumers to grant different levels of access and different usage rights of personal data to different data controllers in different contexts [18, 57].

The theory does not explicitly address the supply of transparency enhancing information (a). The focus is on privacy management of the individual data subject (b). Providing information on personal data processing is a way to support privacy management (c). The time of providing information is not addressed in the theory (d).

Theory of Contextual Integrity

Nissenbaum's **Theory of Contextual Integrity** frames privacy in terms of personal information flows. She calls for not simply restricting the flow of personal information but ensuring that it flows appropriately. She introduces the framework of contextual integrity for determining appropriateness. The framework includes factors determining when people will perceive information technologies and systems as threats to privacy. It helps to predict how people will react to such systems [38–41]. Barth et al. formalized essential elements of contextual integrity in a framework to support technical implementation of data protection requirements [7].

In her paper "A Contextual Approach to Privacy Online" [40], Nissenbaum maintains that the so-called notice-and-consent (or transparency-and-choice) approach has failed. She defines transparency as "conveying information handling practices in ways that are relevant and meaningful to the choices individuals must make" [40]. She claims that in most contexts data subjects are either provided with too little or too much or to detailed information and thus cannot easily make informed decisions (a, b). The focus of the theory is on providing appropriate information on personal information flows. Since the question of what is appropriate also depends on personal characteristics of the data subjects, these are also taken into account. In a broader sense, the appropriateness of transparency-enhancing information for supervising authorities can be considered, too (c). The time at which information is made available is not explicitly addressed in the Theory of Contextual Integrity. However, time is an essential element of appropriate information on personal information flows (d).

Procedural Fairness Theory / Procedural Justice

The **Procedural Fairness Theory**, also known as procedural justice, deals with the perception of individuals *whether a procedure is fair and complies with specified rules*.

[20, 34]. The Procedural Fairness Theory was adapted to privacy by Culnan and Armstrong. When a company's privacy practices are considered questionable and customers suspect misuse of their personal data, they feel being treated unfairly and are unwilling to disclose additional personal data [10].

The adaption of Procedural Fairness Theory to privacy is used by Greenaway et al. [19] in their "Company information privacy orientation (CIPO) framework". They also build on Agency Theory and the Privacy Calculus. The authors use two dimensions to distinguish four company information privacy orientations: (1) control "as a way to differentiate how and the extent to which organisations offer their customers the ability to make choices about how their information is collected, used and reused" (p. 584) and (2) procedural justice which "emphasises the extent to which organisations offer transparency to their customers" (p. 584). The second dimension addresses supplying information on personal data processing to customers (a). The parties involved are the costumer as data subject and the company as data controller (b). The CIPO-Framework is a strategy model that focuses on providing information to customers (c). The authors did not examine the point in time when transparency-enhancing information is presented (d).

Social Contract Theory, Privacy Calculus, Extended Privacy Calculus, Dual Calculus, Utility-maximization Theory

The **Social Contract Theory** was adapted to the privacy context by Milne and Gordon [35]. It assumes that disclosing personal data to an organisation can be regarded as a *social exchange* besides the economic exchange. The resulting social contract is considered fair by the data subject if she/he retains *control* over her/his data. The *cost/benefit analysis* a consumer as data subject makes in entering the social contract leads to a *decision about disclosing personal data*. This *calculus of behavior* by Laufer and Wolfe [32] later was called **Privacy Calculus** [10]. Adapted to e-commerce transactions, Dinev and Hart developed the **Extended Privacy Calculus** [13]. Li proposed an integrated framework named **Dual Calculus** based on the Privacy Calculus and taking a *Risk Calculus* into account [33].

Utility-maximization Theory is based on economic exchange theories. Applied to privacy, it assesses how the overall benefit or satisfaction of a person in terms of data protection can be maximised. The *decision to disclose personal data* is a function of the difference between *expected benefits* (e.g. personalised services) and *expected costs* (e.g. privacy losses). Individuals strive for achieving an appropriate optimum [50]. These utility function is usually referred to as Privacy Calculus [33].

Social Contract Theory, Privacy Calculus, Extended Privacy Calculus, Dual Calculus and Utility-maximization Theory are closely connected to each other. Several authors combine two or more of these theories in information privacy research. For this reason, we assess these theories together using the following examples.

Awad and Krishnan [6] use the Utility-maximization Theory and the Privacy Calculus to explore the "relationship between information transparency and consumer willingness to partake in personalization" [6] (a). The authors concentrate on utility functions of data subjects (b). Awad and Krishnan [6] consider providing information and individual traits of data subjects. They focus on the effect of *privacy concerns*, *former*

privacy invasion experiences and other factors on the *importance of information transparency* and willingness to be profiled online (c). The time of information availability is not taken into account (d).

Dinev et al. [14] build their research on the Privacy Calculus and Procedural Fairness Theory. They study the effect of "importance of information transparency" (defined as in [6]) and "regulatory expectations" (data protection provisions) on perceived risk. The theoretical framework takes the importance of PDT into account (a), concentrating on the individual's behaviour (b, c) but not on the time of information availability (d).

3 Conclusion

In our study, we have found that 42 out of 157 papers, i.e. only about a quarter, mention a theory. Yet, our literature review has revealed several theories that scholars have used to explore PDT. Some authors base their research not only on one theory, but combine different theories into a new research construct. None of the authors identified in our literature review has developed a specific theory for PDT or has drawn on a native PDT theory. Although PDT has evolved to a considerable research topic within information privacy research, no native PDT theory seems to have emerged yet. Nevertheless, our assessment shows that there are several theories that can substantially support research into PDT. We have identified papers referring to established theories from other disciplines such as psychology, sociology, economics, information systems and computer science, e.g. Agency Theory, Information Asymmetry and Signaling Theory, the Theory of Reasoned Action (TRA), the Theory of Planned Behavior (TPB), the Reasoned Action Approach, the Technology Acceptance Model, the Theory of Bounded Rationality, Prospect Theory, the Procedural Fairness or Procedural Justice Theory, Social Contract Theory and Utility-maximization Theory. Several authors draw on privacy theories as theoretical foundation, e.g. Information Boundary Theory (IBT), Communication Privacy Management Theory (CMPT), the Restricted Access/Limited Control Theory of Privacy (RALC), the Privacy Calculus, the Extended Privacy Calculus and the Dual Calculus or the Theory of Contextual Integrity (RQ1).

From a characterization of PDT we have deduced the following requirements that a theory for exploring PDT should address:

- supply of information about collection, processing, use or dissemination of personal data,
- data subjects and data controllers,
- the process of providing information or individual traits of data subjects, and
- the point in time at which information is made available.

Supply of information about collection, processing, use or dissemination of personal data is addressed by all theories with the exception of the Theory of Bounded Rationality, Prospect Theory and the Restricted Access/Limited Control Theory of Privacy (RALC).

Most theories focus on data subjects only. In the context of PDT, these theories help to explore which forms of PDT result in which disclosure willingness or actual disclosure of personal data. It is noticeable that the vast majority of the theories do not even

consider other parties involved. However, an appropriate theory of PDT would take into account not only the data subject but data controllers, data processors, third parties and supervising authorities, since they must at least be involved in providing PDT. Agency Theory, Information Asymmetry, Signaling Theory, the Theory of Contextual Integrity and the "Company information privacy orientation framework" introduced by Greenaway et al. [19] could provide clues for further research in this area.

The process of providing information about collection, processing, use or dissemination of personal data from the data controller to the data subject is addressed by Agency Theory, Information Asymmetry and Signaling Theory, Information Boundary Theory (IBT), Communication Privacy Management Theory (CMPT), The Restricted Access/Limited Control Theory of Privacy (RALC), the Theory of Contextual Integrity, the Procedural Fairness Theory / Procedural Justice and the research approach by Awad and Krishnan [6]. All the other theories focus on individual traits of data subjects.

The point in time at which information is made available by the data controller to data subjects is addressed by only very few theories, namely, the Reasoned Action Approach (RAA), the Theory of Bounded Rationality, and the Theory of Contextual Integrity.

It is also striking that previous research has mainly taken ex-post and ex-ante transparency into account. In this context Adjerid et al. point out "the need to expand the concept of transparency to … making … privacy risks salient and readily available to consumers when they most require them, at the point of disclosure" [2]. Adjerid et al. refer here to an aspect of transparency that we call real-time transparency, i.e. PDT at the time of the decision to disclose personal data. This facet of PDT is probably particularly interesting. However, it has been neglected in previous research and, unfortunately, we have not identified a single theory that could support research in this area (RQ 2).

Only few theories address potential drawbacks of PDT, i.e. the presumption that enhanced PDT may lead to less information privacy. Nissenbaum has explicitly addressed this issue [40] and presented the Theory of Contextual Integrity that may help to further explore this challenge for information privacy research and practice.

Our assessment provides an overview of theories that are used in the context of PDT. However, we do not claim that our study is comprehensive. We have only included papers in our research that explicitly explore PDT and label research foundations with the string "theor*". Our study is based on the assumption that a theory is present when the author of the paper in question uses the term "theory". However, the concept of theory is ambiguous and ambivalent. Therefore, we may have included constructs that are not considered theories in some research disciplines. Furthermore, we have excluded some theories from our study which, in our opinion, do not fit into our research context. Some of these theories, e.g. the Theory of Cryptography, may be relevant for privacy research but not for research into PDT.

Scholars from a wide range of scientific disciplines, e.g. computer science, information systems, privacy, law and media science, have contributed to exploring PDT. Consequently, PDT can most likely not be explored on the basis of a single theory alone. However, research on PDT may build on several theories that open up different perspectives and enable various fields of study.

References

1. Acquisti, A., Adjerid, I., Brandimarte, L.: Gone in 15 Seconds: The Limits of Privacy Transparency and Control. IEEE Secur Priv **11**, 72–74 (2013). doi: 10.1109/MSP.2013.86
2. Adjerid, I., Acquisti, A., Brandimarte, L., Loewenstein, G.: Sleights of Privacy. Framing, Disclosures, and the Limits of Transparency. In: Cranor, L.F., Bauer, L., Beznosov, K. (eds.) SOUPS Proceedings, pp. 1–17 (2013). doi: 10.1145/2501604.2501613
3. Ajzen, I.: The theory of planned behavior. Organ Behav Hum Dec **50**, 179–211 (1991). doi: 10.1016/0749-5978(91)90020-T
4. Ajzen, I., Fishbein, M.: Understanding attitudes and predicting social behavior. Prentice-Hall, Englewood Cliffs, N.J (1980)
5. Altman, I.: The environment and social behavior. Privacy, personal space, territory, crowding. Brooks-Cole Publishing Co, Monterey, CA (1975)
6. Awad, N.F., Krishnan, Mayuram S.: The Personalization Privacy Paradox: An Empirical Evaluation of Information Transparency and the Willingness to Be Profiled Online for Personalization. MIS Q **30**, 13–28 (2006). doi: 10.2307/25148715
7. Barth, A., Datta, A., Mitchell, J.C., Nissenbaum, H.: Privacy and contextual integrity: framework and applications. In: IEEE Symposium on Security and Privacy, 184-198 (2006). doi: 10.1109/SP.2006.32
8. Brandimarte, L., Acquisti, A., Loewenstein, G.: Misplaced Confidences. Privacy and the Control Paradox. Soc Psychol Pers Sci **4**, 340–347 (2013). doi: 10.1177/1948550612455931
9. Cabinakova, J., Zimmermann, C., Müller, G.: An Empirical Analysis of Privacy Dashboard Acceptance: The Google Case. In: ECIS Proceedings (2016)
10. Culnan, M.J., Armstrong, P.K.: Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. Organ Sci **10**, 104–115 (1999). doi: 10.1287/orsc.10.1.104
11. Davis, F.D.: Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. MIS Q **13**, 319 (1989). doi: 10.2307/249008
12. Dinev, T., Bellotto, M., Hart, P., Russo, V., Serra, I., Colautti, C.: Privacy calculus model in e-commerce – a study of Italy and the United States. Eur J Inf Syst **15**, 389–402 (2006). doi: 10.1057/palgrave.ejis.3000590
13. Dinev, T., Hart, P.: An extended privacy calculus model for E-commerce transactions. Inform Syst Res **17**, 61–80 (2006)
14. Dinev, T., Xu, H., Smith, J.H., Hart, P.: Information privacy and correlates: an empirical attempt to bridge and distinguish privacy-related concepts. Eur J Inf Syst **22**, 295–316 (2013). doi: 10.1057/ejis.2012.23
15. Eisenhardt, K.M.: Agency Theory. An Assessment and Review. Acad Manage Rev **14**, 57 (1989). doi: 10.2307/258191
16. Fischer-Hübner, S., Hoofnagle, C., Krontiris, I., Rannenberg, K., Waidner, M., Bowden, C.: Online Privacy: Towards Informational Self-Determination on the Internet. In: Hildebrandt, M., O'Hara, K., Waidner, M. (eds.) Digital Enlightenment Yearbook 2013, pp. 123–138. IOS Press, Amsterdam (2013)
17. Fishbein, M., Ajzen, I.: Predicting and Changing Behavior. The Reasoned Action Approach. Psychology Press, New York (2010)

18. Fuchs, C.: Towards an alternative concept of privacy. Journal of Information, Communication and Ethics in Society **9**, 220–237 (2011). doi: 10.1108/14779961111191039
19. Greenaway, K.E., Chan, Y.E., Crossler, R.E.: Company information privacy orientation. A conceptual framework. Info Systems J **25**, 579–606 (2015). doi: 10.1111/isj.12080
20. Greenberg, J.: A Taxonomy of Organizational Justice Theories. Acad Manage Rev **12**, 9–22 (1987). doi: 10.5465/AMR.1987.4306437
21. Gregor, S.: The Nature of Theory in Information Systems. MIS Q **30**, 611–642 (2006). doi: 10.2307/25148742
22. Hansen, M.: Marrying Transparency Tools with User-Controlled Identity Management. In: Fischer-Hübner, S., Duquenoy, P., Zuccato, A. et al. (eds.) The Future of Identity in the Information Society, 262, pp. 199–220. Springer US, Boston, MA (2008). doi: 10.1007/978-0-387-79026-8_14
23. Hansen, M.: Top 10 Mistakes in System Design from a Privacy Perspective and Privacy Protection Goals. In: Camenisch, J., Fischer-Hübner, S., Rannenberg, K. (eds.) Privacy and Identity 2011, IFIP AICT 375, pp. 14–31. Springer Berlin Heidelberg (2012). doi: 10.1007/978-3-642-31668-5_2
24. Hauff, S., Dytynko, O., Veit, D.: The Influence of Privacy Dispositions on Perceptions of Information Transparency and Personalization Preferences. In: Proceedings of the 50th Hawaii Intern. Conference on System Sciences, pp. 5006–5015. AIS Electronic Library (AISeL) (2017). doi: 10.24251/HICSS.2017.607
25. Heath, J.: Contemporary Privacy Theory Contributions to Learning Analytics. JLA **1**, 140–149 (2014). doi: 10.18608/jla.2014.11.8
26. Hildebrandt, M.: The Dawn of a Critical Transparency Right for the Profiling Era. In: Bus, J., Crompton, M., Hildebrandt, M. et al. (eds.) Digital enlightenment yearbook 2012. IOS Press, Amsterdam, Washington, D.C. (2012)
27. Hildén, J.: The normative shift: Three paradoxes of information privacy. In: Kramp et al. (ed.) Politics, civil society and participation. Media and communications in a transforming environment, pp. 63–73. edition lumière, Bremen (2016)
28. Ifenthaler, D., Schumacher, C.: Student perceptions of privacy principles for learning analytics. ETR&D-Educ Tech Res **64**, 923–938 (2016). doi: 10.1007/s11423-016-9477-y
29. Kahneman, D., Tversky, A.: Prospect Theory. An Analysis of Decision under Risk. Econometrica **47**, 263 (1979). doi: 10.2307/1914185
30. Karwatzki, S., Dytynko, O., Trenz, M., Veit, D.: Beyond the Personalization–Privacy Paradox. Privacy Valuation, Transparency Features, and Service Personalization. J Manage Inform Syst **34**, 369–400 (2017). doi: 10.1080/07421222.2017.1334467
31. Kowatsch, T., Maass, W.: Critical Privacy Factors of Internet of Things Services: An Empirical Investigation with Domain Experts. In: Rahman, H. (ed.) Knowledge and technologies in innovative information systems. (MCIS 2012), pp. 200–211. Springer, Berlin (2012). doi: 10.1007/978-3-642-33244-9_14
32. Laufer, R.S., Wolfe, M.: Privacy as a Concept and a Social Issue. A Multidimensional Developmental Theory. J Soc Issues **33**, 22–42 (1977). doi: 10.1111/j.1540-4560.1977.tb01880.x
33. Li, Y.: Theories in online information privacy research. A critical review and an integrated framework. Decis Support Syst **54**, 471–481 (2012). doi: 10.1016/j.dss.2012.06.010

34. Lind, E.A., Tyler, T.R.: The Social Psychology of Procedural Justice. Plenum Pr, New York, NY (1988)
35. Milne, G.R., Gordon, M.E.: Direct Mail Privacy-Efficiency Trade-offs Within an Implied Social Contract Framework. J Public Policy Mark **12**, 206–215 (1993)
36. Monteleone, S.: Addressing The 'Failure' Of Informed Consent In Online Data Protection: Learning the Lessons From Behaviour-aware Regulation. Syracuse Journal of International Law & Commerce **43**, 69–119 (2015)
37. Murmann, P., Fischer-Hübner, S.: Tools for Achieving Usable Ex Post Transparency. A Survey. IEEE Access **5**, 22965–22991 (2017). doi: 10.1109/ACCESS.2017.2765539
38. Nissenbaum, H.: Privacy as contextual integrity. Wash Law Rev **79**, 119–158 (2004)
39. Nissenbaum, H.: Privacy in Context. Technology, Policy, and the Integrity of Social Life. Stanford Law Books an imprint of Stanford University Press, Stanford, CA (2010)
40. Nissenbaum, H.: A Contextual Approach to Privacy Online. Daedalus **140**, 32–48 (2011). doi: 10.1162/DAED_a_00113
41. Pardo, A., Siemens, G.: Ethical and privacy principles for learning analytics. Br J Educ Technol **45**, 438–450 (2014). doi: 10.1111/bjet.12152
42. Petronio, S.: Communication Boundary Management. A Theoretical Model of Managing Disclosure of Private Information Between Marital Couples. Commun Theory **1**, 311–335 (1991). doi: 10.1111/j.1468-2885.1991.tb00023.x
43. Petronio, S.S.: Boundaries of privacy. Dialectics of disclosure. State University of New York Press, Albany (2002)
44. Pollach, I.: Privacy Statements as a Means of Uncertainty Reduction in WWW Interactions. Journal of Organizational & End User Computing **18**, 23–48 (2006)
45. Pope, J.A., Lowen, A.M.: Marketing implications of privacy concerns in the US and Canada. Direct Marketing: An International Journal **3**, 301–326 (2009). doi: 10.1108/17505930911000883
46. Publications Office of the European Union: General Data Protection Regulation. 2016/679 (2016)
47. Rader, E.: Awareness of Behavioral Tracking and Information Privacy Concern in Facebook and Google. In: SOUPS Proceedings, pp. 51–67. USENIX (2014)
48. Roeber, B., Rehse, O., Knorrek, R., Thomsen, B.: Personal data: how context shapes consumers' data sharing with organizations from various sectors. Electron Markets **25**, 95–108 (2015). doi: 10.1007/s12525-015-0183-0
49. Rowe, F.: What literature review is not. Diversity, boundaries and recommendations. Eur J Inf Syst **23**, 241–255 (2014). doi: 10.1057/ejis.2014.7
50. Rust, R.T., Kannan, P.K., Peng, N.: The customer economics of internet privacy. J Acad Market Sci **30**, 455–464 (2002). doi: 10.1177/009207002236917
51. Simon, H.A.: A Behavioral Model of Rational Choice. The Quarterly Journal of Economics **69**, 99 (1955). doi: 10.2307/1884852
52. Simon, H.A.: Theories of Decision-Making in Economics and Behavioural Science. Palgrave Macmillan UK (1966)
53. Spence, M.: Job Market Signaling. The Quarterly Journal of Economics **87**, 355 (1973). doi: 10.2307/1882010
54. Stutzman, F., Capra, R., Thompson, J.: Factors mediating disclosure in social network sites. Comput Hum Behav **27**, 590–598 (2011). doi: 10.1016/j.chb.2010.10.017

55. Sutton, R.I., Staw, B.M.: What Theory is Not. Admin Sci Quart **40**, 371 (1995). doi: 10.2307/2393788
56. Tavani, H.T.: Philosophical Theories of Privacy. Implications for an adequate online privacy policy. Metaphilosophy **38**, 1–22 (2007). doi: 10.1111/j.1467-9973.2006.00474.x
57. Tavani, H.T.: Informational Privacy. Concepts, Theories, and Controversies. In: Himma, K., Tavani, H.T. (eds.) The handbook of information and computer ethics, pp. 131–164. Wiley, Hoboken, N.J (2008). doi: 10.1002/9780470281819.ch6
58. Tavani, H.T., Moor, J.H.: Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. SIGCAS Comput. Soc. **31**, 6–11 (2001). doi: 10.1145/572277.572278
59. Tene, O., Polenetsky, J.: To Track or "Do Not Track". Advancing Transparency and Individual Control in Online Behavioral Advertising. Minn. JL Sci. & Tech. **13**, 281 (2012)
60. Tversky, A., Kahneman, D.: Judgment under Uncertainty. Heuristics and Biases. Science **185**, 1124–1131 (1974). doi: 10.1126/science.185.4157.1124
61. Tversky, A., Kahneman, D.: The framing of decisions and the psychology of choice. Science **211**, 453–458 (1981). doi: 10.1126/science.7455683
62. Walker, K.L.: Surrendering Information Through the Looking Glass: Transparency, Trust, and Protection. J Public Policy Mark **35**, 144–158 (2016)
63. Warren, S.D., Brandeis, L.D.: The Right to Privacy. Harvard Law Rev **4**, 193 (1890). doi: 10.2307/1321160
64. Webster, J., Watson, R.T.: Analyzing the Past to Prepare for the Future. Writing a Literature Review. MIS Q **26**, xiii–xxiii (2002)
65. World Economic Forum: Rethinking Personal Data: A New Lens for Strengthening Trust. Cologny/Geneva (2014)
66. Zhang, B., Xu, H.: Privacy Nudges for Mobile Applications: Effects on the Creepiness Emotion and Privacy Attitudes. In: Proceedings of the 19th ACM Conference on Computer-Supported Cooperative Work & Social Computing, pp. 1676–1690. ACM, San Francisco, CA (2016). doi: 10.1145/2818048.2820073