sustainability

MDPI

Article

Motivating Users to Manage Privacy Concerns in Cyber-Physical Settings—A Design Science Approach Considering Self-Determination Theory

Sabrina Oppl and Christian Stary *

Business Informatics-Communications Engineering, Business School, Johannes-Kepler University of Linz, 4040 Linz, Austria; sabrina.oppl@jku.at
* Correspondence: christian.stary@jku.at

Abstract: Connectivity is key to the latest technologies propagating into everyday life. Cyber-Physical Systems (CPS) and Internet-of-Things (IoT) applications enable users, machines, and technologically enriched objects ('Things') to sense, communicate, and interact with their environment. Albeit making human beings' lives more comfortable, these systems collect huge quantities of data that may affect human privacy and their digital sovereignty. Engaging in control over individuals by digital means, the data and the artefacts that process privacy-relevant data can be addressed by Self-Determination Theory (SDT) and its established instruments. In this paper, we discuss how the theory and its methodological knowledge can be considered for user-centric privacy management. We set the stage for studying motivational factors to improve user engagement in identifying privacy needs and preserving privacy when utilizing or aiming to adapt CPS or IoT applications according to their privacy needs. SDT considers user autonomy, self-perceived competence, and social relatedness relevant for human engagement. Embodying these factors into a Design Science-based CPS development framework could help to motivate users to articulate privacy needs and adopt cyber-physical technologies for personal task accomplishment.

Keywords: digital privacy; digital sovereignty; Design Science; Self-Determination Theory; Cyber-Physical System; method appropriation; user engagement; Internet-of-Things

check for updates

Citation: Oppl, S.; Stary, C. Motivating Users to Manage Privacy Concerns in Cyber-Physical Settings—A Design Science Approach Considering Self-Determination Theory. *Sustainability* **2022**, *14*, 900. https://doi.org/10.3390/su14020900

Academic Editors: Miltiadis D. Lytras, Anna Visvizi and Anastasija Nikiforova

Received: 29 December 2021
Accepted: 10 January 2022
Published: 13 January 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

Currently, Cyber-Physical Systems (CPS) and thereby, Internet-of-Things (IoT) applications, have become increasingly common in production and service industries, as well as in private households and everyday life. To consider the vast amount of components or 'things' propagating to the Internet that aid society in becoming connected, one must also consider the way in which these components are related to the privacy of users, either in terms of data or steadiness of connection. CPS and their components' privacy-relevant data, such as personal data, are collected and can be used by other applications and providers of services, e.g., creating company and person-related profiles, to complement other business. Besides security, interoperability, and other technology-related challenges (cf. [1]), privacy of users is considered crucial, as data are collected and utilized in many cases without the explicit agreement of humans [2,3]. Such a course of action may have unintended consequences, for both individuals and the organizations collecting the data, due to further processing and distribution of data.

In this article, we understand privacy in line with Art. 12 of The Universal Declaration of Human Rights (https://www.un.org/sites/un2.un.org/files/udhr.pdf (accessed on 2 December 2021)); that users of CPS and IoT applications should not be subjected to arbitrary interference with their privacy. Privacy means 'freedom from unauthorized intrusion: state of being let alone and able to keep certain especially personal matters to oneself' (https://www.merriam-webster.com/dictionary/privacy#legalDictionary (accessed on

2 December 2021)). In particular, keeping personal matters to oneself indicates the control and self-determined decision on matters when interacting with technologies, such as CPS and IoT applications. Freedom from unauthorized intrusion addresses the interference into matters by means of technology, and aims to make sure that technology cannot disturb user matters that the individual decides to remain personal.

Maintaining privacy means avoidance of unjustifiable intrusion into the private space of a user 'by appropriating his or her name or likeness, by unreasonably interfering with his or her seclusion, by publicizing information about his or her private affairs that a reasonable person would find objectionable and in which there is no legitimate public interest, or by publicizing information that unreasonably places him or her in a false light' (https://www.merriam-webster.com/legal/invasion%20of%20privacy (accessed on 2 December 2021)). This explanation is of twofold interest. On the one hand, it details the privacy-relevance of data. Hence, privacy management not only concern private data, but also interpretations and judgments on persons. The understanding of private data does not reflect that entirely, as it is understood as being any information 'that reveals racial and ethnic origin, political, philosophical, religious opinions or trade union affiliation, or that concern life or health, or that concern sex life or health, including the genetic data' (https://www.un.org/sites/un2.un.org/files/udhr.pdf (accessed on 2 December 2021)).

On the other hand, the explanation refers to justification when privacy-relevant data are concerned. Hence, users need to be informed by giving a reason when privacy-relevant data are collected, processed, or shared by technologies, including interpretations and judgements. According to Art. 8 of the European Convention on Human Rights (https://www.echr.coe.int/Pages/home.aspx?p=basictexts/convention (accessed on 2 December 2021)) persons have the general right to respect of their privacy in terms of a secured space in which a person pursues their individual personal interests. Hence, the right to privacy concerns self-determination with respect to one's lifestyle, aiming for the physical and mental integrity of a person, for example regarding their gender identity and other social relationships [4]. In Art. 29 par. 2 of The Universal Declaration of Human Rights, self-determination is addressed implicitly through the following statement, 'in the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society' (https://www.un.org/sites/un2.un.org/files/udhr.pdf (accessed on 2 December 2021)). Hence, besides the right to confidentiality of communication, the right to be left alone, and thus, to control one's own life, and the right to protect one's personal data are crucial in preserving privacy in the IoT age [5].

Regulations have been developed that enable people to protect themselves against interference or Interventions in their private sphere, such as the EU's General Data Protection Regulation (GDPR) (http://gdpr.eu (accessed on 2 December 2021)). This is an example of how digital sovereignty could manifest in everyday life. However, the approach is still debated on whether the proposed rules are applicable in practice [6]. Under the threat of punitive sanctions, any organization must abide by a set of data management rules if it wants to trade with customers in EU countries. Those rules make it possible for individual citizens to take more control of how their data are used, and they also set potential fines for if companies breach the regulations. Hence, connected Things require justification for sending and collecting data related to a person's privacy. Users need to know that they are sending their data and must be aware to whom exactly and for which purpose. For example, while installing a home healthcare application on a smart phone, users need to be informed on these issues and finally accept the conditions of privacy-relevant data collection and sharing.

In this way, the role of users changes constantly. For each highly connected service, information has to be studied on privacy, decisions have to be taken, and finally, informed consent has to be given. When users engage in privacy management, they determine the collection and use of data related to their privacy. Still, user engagement in privacy management of private users is hindered, partly due to misconceptions and partly due to technic-centricity [7–9]. Misconceptions lead to misunderstandings with respect to data collection and processing, e.g., when giving consent to cookies or cross-application access. Technic-centricity refers to terms and concepts, such as cookie, that do not have a corresponding definition in the user environment.

In general, people's engagement in activities is determined by their motivation [10]. The authors of [10] state that motivation 'is therefore of preeminent concern to those [. . .] that involve mobilizing others to act.' Self-Determination Theory (SDT) addresses motivation and engagement by describing different types and qualities of motivation. Furthermore, SDT describes factors influencing people's motivation to act [11]. Privacy management issues have only recently been addressed in SDT research, namely in the context of cloud storage [12]. In this paper, we take this initial work as input for further SDT-driven research, as it helps to manifest privacy management as a socio-technical topic based on empirically valid results. With our work, we want to set the stage for SDT-informed privacy management research and privacy management features that motivate users to adapt technologies according to their privacy needs.

The resulting research question is: How can privacy management research and development be informed by Self-Determination Theory, so that humans are motivated to engage in adopting the respective application features?

We suggest a Design Science [13] approach to structure user-centric privacy management developments. We identify fundamental design cycles to utilize SDT instruments according to their multiple facets for design and evaluation. SDT-driven development in this way can contribute to both analyzing and supporting user engagement in their privacy management in the digital world. As an effect, future developments in privacy management can take into account the basic psychological needs addressed by SDT in a balanced and well-structured way, namely the perceived competence of (potential) users, their autonomy in managing their privacy, and social relatedness as caretaker of personal privacy needs.

In Section 2 we review existing research on user-centric privacy management, in order to reflect on the changing role of users and its current involvement in privacy management activities. We derive requirements for user-centric privacy management (development) from existing research. In Section 3 we introduce the fundamental concepts and instruments of SDT. In Section 4 we integrate SDT-based design and development into Design Science-based development cycles. We exemplify how methodological SDT development (https://selfdeterminationtheory.org/questionnaires/ (accessed on 2 December 2021)) could be utilized to support user-centric privacy management. Section 5 concludes the paper by reflecting on the proposed development scheme for further work.

2. Towards User-Centric Privacy Management

In this section we review existing findings on user involvement and engagement policies in privacy management, in particular the adoption of privacy management features of IoT systems and CPS. We also reflect on the aspect of the self-organization of privacy issues as part of information self-determination. We first review current techniques for privacy preservation and user-related concerns of privacy management. Then, we revisit common features of privacy management stemming from technology use. Finally, we analyze existing approaches to contextualize IoT system and CPS development, capturing information relevant for user-centric development. A list of corresponding requirements for user-centric development completes the section.

2.1. The Shift from Techno- to User-Centric Privacy Awareness

There is a significant amount of research in the area of privacy preservation. As recently shown by Alimutiari et al. [14], several mechanisms have been proposed with the goal of how users can benefit from IoT applications while taking into account privacy issues.

As the list reveals, among the proposed methods for privacy preservation, technological means dominate (14, p. 417):

- *Encryption*: This concerns data that are encrypted between the sending parties, e.g., the user and the receiving party, e.g., an IoT device provider, assuming the receiver is a trusted party.
- *Dummy Request*: This mechanism adds some effort to communication on the user side—some fake requests are sent in addition to the actual ones to mislead parties, aiming to intrude the user's privacy.
- *Obfuscation*: In this case, some noise is added to data or other changes are made, such as complementing information or decomposing messages, in order to conceal the location within a certain area and hinder its recognition through data changes.
- *Cooperation*: This technique hides a single request through mashing it with a group of other requests. They are sent by other users from a certain region, without a need to communicate with the receiver. Sending all requests at once, the identity could be hidden within the group of cooperating users.
- *Trusted Third Parties* (TTP): An intermediate component, e.g., server system, is used to hide the identity of users when communicating further; again, assuming this intermediate component can be trusted with respect to preserving privacy.
- *Privacy Information Retrieval* (PIR): This technique hides the actual request in a large amount of information. Much more information is requested than originally required by a sender.

These technology-driven mechanisms process several privacy-relevant categories of data [15], in particular the following ones:

1. *Location awareness data* enables tracking, and thus disclosing a person's or a personal component of the location to others.
2. *Identity information* is collected when data refer to their owner, so any malicious part could intercept it.
3. *Profile* as information about individuals is compiled to infer interests by correlation with other user profiles and exchanged data.
4. *Linkage* occurs in the background, when a provider or architecture component puts into mutual context different system components and user activities.
5. *Exchanged data* concern data exchanged between IoT components due to their connectivity. As the data can be assigned to persons due to the roles of 'sender' and 'receiver', they can be attained and shared. Privacy-relevant information refers to these data.

Collecting and processing the various categories of privacy-relevant data has raised privacy concerns of users, and finally led to considering privacy from a user-centric perspective, e.g., Skarmeta et al. [16]. User-centered privacy management should help to overcome the recognized lack of awareness and intensify the privacy-by-design of IoT applications, and thus increase user motivation to become involved in privacy management. The goal of user-centric privacy management is that individuals, communities, and organizations can determine for themselves when, how, and to what extent information about them is communicated to others. Thereby, privacy requirements can either stem from user-specific situations, e.g., operating a home healthcare CPS, or from regulatory bodies, e.g., healthcare authorities, that need to be met when using CPS services.

2.2. User Engagement and Self-Determination

Kounoudes et al. [17] investigated user-centric IoT studies on privacy (based on [18]), published in the period from 2010 to 2019, because studies near or prior to 2010 were mostly service or provider-oriented, instead of user-centric. The studies addressed privacy concerns in IoT, followed a user-centric approach, and provided a privacy protection solution. The role of users with respect to the characteristics of the GDPR (http://gdpr.eu (accessed on 15 December 2021)—see also introduction) and the implementation of data privacy-by-design and by default (Article 25) has been made transparent in 29 papers. Wachter [18] identified four user privacy challenges in GDPR: (1) profiling, inference, and discrimination; (2) control and context-sensitive sharing of identity; (3) consent and uncertainty; and (4) honesty, trust, and transparency. Privacy solutions studied by Kounoudes et al. [17] provided interactive features for the specification of the privacy preferences, using the privacy-by-design principle when creating IoT devices.

Kounoudes et al. [17] identified that most effort has been spent on (3) consent and uncertainty, as informed consent is considered key in enabling users to disclose their data in the IoT without compromising their privacy. Researchers targeted the efficiency of user consent reducing constraints. The analyzed solutions referring to control and identity sharing (2) showed a variety of tools to control and manage personal data, allowing for the implementation of constraints and policies. Features to specify personal privacy preferences, leading to a user profile (1), proved effective in enhancing user privacy. In case the selection of privacy preferences is unclear to users, e.g., due to the pervasive features of IoT and data collection without user perception, users are supported to regulate how their data can be used. Interactive components, such as Personal Data Managers, enable for specifying who can access data and why, or when carrying out specific actions on the data.

Typical privacy management options are data deletion or rectification. They may be triggered when a user receives a notification on some privacy preferences or risk. Dedicated assistance or coaching components can provide context information, including whether surrounding IoT resources have user-configurable settings. An active privacy management component enables users to determine how IoT devices can take actions for them, enforcing privacy preferences before any user interaction occurs with IoT services or components. Risk estimation typically considers the user profile, the context, and the user's trust in the third party, because privacy risks are closely related to inferences on collected data. Because the privacy risks of data collection have a potential impact of a privacy breach incident, a solution is to notify the users about them, and provide recommendations to the user regarding which personal data should not be shared after estimating the risks of data collection. These mechanisms should help to build trust due to transparent processing (4).

The development of digital identities to handle user privacy has been considered key in the context of interconnected devices. The developed service-oriented frameworks and tools which 'distill privacy-related digital identity requirements (business interoperability) into a set of services, which in turn can be implemented on the basis of open standards (technical interoperability)' [19] still require highly informed users. Research and development should recognize heterogeneously subjective perceptions of privacy by users, and their right to informational self-determination [20].

Active user involvement is required from an awareness and tool perspective involving risk communication. It concerns granular and usable information, as well as informed privacy protection decision support [20]. The active involvement of the user targets the user capability of building an individual mental model of the control mechanism and the preservation of privacy [21,22]. This model decides whether a user trusts or mistrusts a system. It requires transparency and intelligibility of user control mechanisms—see also Figure 1.

Figure 1 shows the various contextual factors that need to be recognized when a user is operating in an environment where privacy issues are managed, and should lead to trusted interaction with a system. The factors include the domain or work scenario a user is part of, goal setting with respect to privacy, the relation to other domains such as security and risk management, and finally, the mindset and set of skills for informed decision-making on privacy-relevant topis. According to Feth et al. [21], the most essential part of user involvement is the creation of personas addressing all user groups in order to better understand the users and their privacy goals. In cooperation with the user, several privacy goals need to be achieved:

1. Unlinkability, in order to ensure that personal data cannot be elicited nor processed, nor used for purposes other than those explicitly specified.

2. Intervenability, in order to enable all concerned people have control through system access, and thus, to enforce their legal rights accordingly.
3. System transparency, concerning the processing of personally identifiable information, in a verifiable and assessable way.

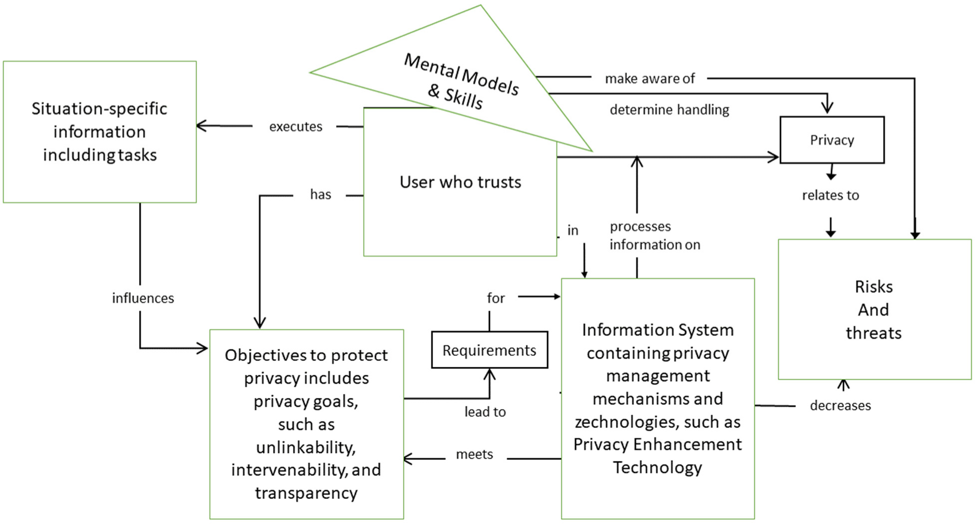
Situation-specific information including tasks
executes
Mental Models & Skills
make aware of
determine handling
Privacy
User who trusts
has
relates to
in
processes information on
Risks And threats
influences
for
Information System containing privacy management mechanisms and zechnologies, such as Privacy Enhancement Technology
Requirements
Objectives to protect privacy includes privacy goals, such as unlinkability, intervenability, and transparency
lead to
decreases
meets

Figure 1. User characteristics in privacy management and technology context according to [21].

Based on participatory design of use cases, a conceptual system model and mechanisms for continuous transparency management can be developed. Thereby, the user's mental model needs to be consistent with the behavior of the system. For each system component, the user's skills and knowledge need to be checked. The aim is to ensure user understanding of how the system helps to achieve privacy goals and requirements.

In a collaborative process, the continuous visibility of the system's states and user's actions with respect to privacy requirements are evaluated. Thereby, system transparency is checked in terms of matching the current state of the system and the interactions with user intentions, (required) actions, and resulting effects. The level of abstraction and granularity of information needs to be determined in collaboration, taking into account user reactions and feedback to designs when operating the system.

Knijnenburg et al. [23] suggest considering user-centric privacy management beyond transparency and control, while Janssen et al. [8] argues in the direction of self-determination when suggesting the improvement of decision-making support. Once it comes to solve real-world privacy problems, as IoT applications become widely used in everyday life, such as households, privacy research should tackle decision processes. They are assumed to have a transformatory effect on the difficulty of privacy decisions and the usability of privacy interfaces. Decision-making support also facilitates interpreting vast amounts of information delivered by regulatory bodies and technology providers. Harnessing the provided control requires skills that many users need to have for informed decision-making.

2.3. Facilitating User Engagement

Several tools have been developed to inform users in decision-making on privacy issues. Bracamonte et al. [24] refers to detectors of privacy-sensitive information. Detecting such information requires some ontology on privacy, e.g., as proposed by Li et al. [12], and leads to alerts that trigger decisions on user privacy. Decision-making concerns aggregating and managing their own data, and determining when and with whom these data are shared, either to be consumed or processed [8]. A respective tool has been considered useful by users, albeit their neutral level of intention of using the tool. They shifted the burden of using it to others, while becoming concerned about its effectiveness and the privacy risks when using it. Studying a Corona tracing app, Pape et al. [25] relates privacy to education.

Their evaluations revealed that the more knowledge users have on privacy concerns, the less hindrances they experience in adopting such apps. Hence, education seems to be key for informed decision-making, in particular in special situations such as a pandemic [26].

However, individuals' self-representations may serve well as context for informational self-determination, when privacy indicators are utilized for privacy management [27], as the following citation reveals. "*Privacy indicators aim to help users to understand the privacy implications of a service by showing values of parameters such as what kinds of data are collected, for what purposes and whether the data are shared with third parties. However, such decision support tools rely entirely on the attributes of the app itself while ignoring exogenous aspects of context that may also have an effect. Such factors include the individual's prior perceptions, interactions and relationships with the organisations associated with the service in question*" ([27]. p. 168).

Michael et al. [28] studied user-relevant context factors and developed a context meta-model that has been applied on IoT manufacturing processes, and "*is defined by four contexts. The Personal and Social Context describes all relevant Persons (e.g., in the use case of IoT manufacturing working tasks: workers, managers, administration staff, suppliers) referring to their abilities, mental and physical information about persons, tasks or duties. The Behavior Context addresses the tasks persons do: steps and goals. The Behavior Context consists of an Activity and related Events. Activities are part of a Process with a certain Goal including sub-goals. Goals in our use case are e.g., to produce a certain product, to control a production step or to deliver a component. The Spatial Context represents all concepts related to venues like Departments (i.e., Factory Buildings) that might differ in Locations, within Areas and certain Equipment, which can be placed in these areas. The Environmental Context is highly relevant for our use case, as either the usage of certain Resources (device, application, item, fixture) by persons is stored as well as the behaviour of these resources by using its sensor data. Thing and Modeling Element are the meta-concepts*." ([28], p. 199).

These types of contexts could frame dedicated tools for privacy management, as was suggested by the developers of Privacy Assistant. Stöver et al. [29] show that such an assistant system should support all contexts where a user wants to implement their privacy preferences. User preferences lead to privacy settings that are valid as defined by the user or as discovered in the privacy preferences of a user. The generated outputs are settings the Assistant can enforce for all components that a user can address when implementing privacy requirements, which typically concern IoT devices.

Besides the user as a concerned privacy stakeholder, the provider or developer of a system or component is also key when being connected to the Assistant. A provider can inform about constraints or regulations stemming from the legal organizations. The provider could also be the designer, thus determining whether software, hardware, or social interaction has some privacy-relevant relation to an authority influencing development [27]. More particularly, developers can influence what users actually learn about the purpose and the internal structure of a system, including loopholes to infiltrate systems on demand. Having stated the different roles and their relations, this brings us back to transparency and control, for which developers take responsibility when distributing it between participants.

Control and transparency influence the design of user interfaces that are primarily required to specify privacy settings and communicate with the IoT system through feedback and actions. Hence, the user interface becomes the 'perceptible part of the IoT' [17]. It should allow the user to have a clear understanding of the associated privacy risks through proper encodings, e.g., using annotations when creating inferences about that user. Once a risk alert appears, users can perform corresponding actions, such as data anonymization before sharing, which need to be integrated to ensure user control over personal data. Such a course of action lays ground for informed consent in IoT, as users are kept apprehensive about the fact that their data can be collected and shared. Even in cloud-based IoT applications and dynamically changing contexts, the ability to model the user's privacy preferences is considered a prerequisite to enable the user to make an informed decision (cf. [8]).

In summary, designers and providers need to ensure:

1. *Transparency on data level and inferences* for users to achieve their informed consent;
2. *Preference specification on privacy* as inherent utility function of IoT applications;
3. *Availability of context information* to support decision-making on (i) and (ii);
4. *Control in terms of privacy options setting and monitoring* throughout runtime.

Hence, indirectly all dimensions of self-determination have been addressed in the context of user roles and their activities. User should be able to autonomously decide based on transparent options with what or to whom to share data. Informed decision-making, and, finally, consent, is based on education and competence; thus, addressing users' perceptions of their competence, and of their relatedness to other users, either directly or via the provider, is necessary.

3. Self-Determination Theory

Self-determination Theory (SDT) is "a macro-theory for human motivation, emotion and personality" based on research by Edward Deci and Richard Ryan [30]. In contrast to behavioristic approaches, SDT focuses on "people's inherent motivational propensities for learning and growing, and how they can be supported" instead of controlling motivation exclusively from the outside [11]. However, the pursuit of individual development and the willingness to learn does not arise automatically [11]. The social environment influences how far people engage in activities and what people learn [10].

In this section, we give an overview of the central findings of the SDT to identify potential fields of application in the context of user-centric privacy management in the subsequent section. Because SDT differs between intrinsic and extrinsic motivation, the following subsection describes each type of motivation in the context of self-determination. It is followed by a subsection about three basic needs that must be satisfied to allow for engagement and self-determined motivation.

3.1. Intrinsic Versus Extrinsic Motivation and the Question of Self-Determination

When people act out of interest or fun, their actions are intrinsically motivated [31]. The behavior of children especially is often triggered by interest, fun, or curiosity. However, intrinsic motivation is also evident in adults if activities are carried out for one's own sake. For example, sporting or artistic activities are often based on intrinsic motivation [32]. Thereby, *"Intrinsic motivation is defined as the doing of an activity for its inherent satisfactions rather than for some separable consequence. When intrinsically motivated a person is moved to act for the fun or challenge entailed rather than because of external prods, pressures, or rewards."* [31].

Intrinsically motivated behavior is self-determined because "people understand the activity to be something they want to do for its own sake" [32]. It is usually associated with well-being and high-quality performance [33,34].

Although intrinsic motivation is an important type of motivation, people perform many actions without experiencing inherent satisfaction [31]. Such actions are defined as extrinsically motivated because they are performed to achieve a separable outcome [35], as the following quote shows.

> *"The term extrinsic motivation refers to the performance of an activity in order to attain some separable outcome, and thus, contrasts with intrinsic motivation"* [10].

However, acting to achieve a separable outcome does not necessarily lead to a feeling of being externally controlled [10]. According to SDT, there are different subtypes of extrinsic motivation. They vary in terms of perceived self-determination [32,35].

The perceived self-determination depends on the degree of the internalization of values underlying the behavior [11], as described in the following:

- External Regulation is the least autonomous form of extrinsic motivation and therefore is placed just right after amotivation. This subtype represents the behavior people perform to receive a reward or to avoid negative consequences as punishments [11]. Hence, external regulation corresponds to "the type of motivation focused on by operant theorists" [10].

- Introjection represents the second non-autonomous subtype of extrinsic motivation, although the underlying values have been "partially internalized" [11]. The "behavior is regulated by the internal reward of self-esteem for success and by avoidance of anxiety, shame or guilty for failure" [11]. Thus, people experience an internal pressure to act without identifying with the underlying value, nor do they "accept it as his or her own" [36].
- Identification is a more self-regulated or autonomous form of extrinsic motivation [11]. "Here, the person has identified with the personal importance of a behavior and has thus accepted its regulation as his or her own" [31]. Hence, people have internalized the underlying values and perceive the behavior as somewhat self-determined [11].
- Integration describes the most autonomous or self-regulated subtype of extrinsic motivation [11]. In contrast to identification, a "person not only recognizes or identifies with the value of the activity, but also finds it to be congruent with other core interests and values" [11]. Such autonomous extrinsic motivation shares with intrinsic motivation perceived self-determination [11] and high-quality performance [31].

Hence, high-quality performance, engagement, and persistence is not just a question of intrinsic or extrinsic motivation. "What distinguishes the two is merely a teleological aspect, whether the behavior is done for its inherent satisfaction (intrinsic) or is done in order to obtain a separable goal" [35]. Hence, engagement or performance is a question of perceived self-determination. The internalization of values determines whether people experience extrinsically motivated behavior as controlled or as self-determined [31].

How far people internalize the values of a behavior depends on the satisfaction of their psychological needs [11], which can be fostered or inhibited through the social environment [37]. SDT describes three basic psychological needs that are essential for all humans "across individual and cultural differences" [38]. The following section describes the three basic needs to understand the influencing factors of the internalization process.

3.2. Basic Needs

Numerous studies have shown that all humans have three basic psychological needs: They need to feel competent, autonomous, and a relatedness, for individual growth, engagement, and well-being [11].

The need for **competence** describes that people want to perform activities that optimally meet their abilities. However, it is "not an attained skill or capability, but rather is a felt sense of confidence and effectance in action" [39]. In general, people seek to maintain and improve their skills for personal growth [39]. To achieve this, people need to feel that they can successfully accomplish their tasks [11]. The social environment can facilitate the feeling of competence through "well-structured environments that afford optimal challenges, positive feedback, and opportunities for growth" [11].

The need for **autonomy** describes that people want to perceive the causation of action in themselves [11]. The term "autonomy" refers to "self-governance" [40]; the following quote specifies with respect to these terms,

> *"[. . .] in no way does the idea of self- governance imply, either logically or practically, that people's behavior is determined independently of influences from the social environment [. . .]. We know of no real-world circumstances in which people's behavior is totally independent of external influences, but, even if there were, that is not the critical issue in whether the people's behavior is autonomous. Autonomy concerns the extent to which people authentically or genuinely concur with the forces that do influence their behavior"* [40].

Opportunities of choices can facilitate the feeling of autonomy. However, choices can only have positive effects when they are attributed a personal significance. If people do not perceive the tasks or activities to be chosen as personally relevant, they will not experience any autonomy support [37].

Relatedness is the third basic need and describes how people want to feel connected to others. It also represents the desire to be supported and accepted. People seek to be part of a community with shared interests and values [39]. The social environment can facilitate this psychological need "by conveyance of respect and caring" [11].

These basic needs are essential for both intrinsic and extrinsic motivation. "Thwarting of any of these three basic needs is seen as damaging to motivation and wellness" [11]. In general, intrinsically motivated behavior is based on feeling autonomous and competent because people perform such activities out of joy and interest [32]. Nevertheless, the social environment can reduce intrinsic motivation when basic needs are not considered. For example, controlled environments, rewards, punishments, and negative feedback have negative effects on people's intrinsic motivation [32,41]. For extrinsically motivated behavior, basic needs satisfaction influences the internalization process. Studies have shown that feeling competent, autonomous, and relatedness supports people to transform values into their own. Internalized and integrated values allow for feelings of self-determination that promote engagement, high-quality performance, and well-being [31].

These recent studies on value embodiment demonstrate the positive impact of internalization on individual engagement and serve as a trigger to apply SDT for motivating users to actively manage their privacy management in cyber-physical environments. As Liu et al. [42] could demonstrate, such a drawing upon SDT enables the investigation of the effects of perceived autonomy, perceived competence, and perceived social relatedness on the relation between information assurance and perceived information control. As 'the three psychological needs fully mediate the impact of information assurance on perceived information control' ([42], p. 113), with the latter driving the adoption of technological services, privacy management feature development could be grounded by SDT.

4. Towards Self-Determined Privacy Management

In this section we put the findings detailed in the previous sections into mutual context. According to our objective, we structure the development process for engaging users in privacy management in line with SDT. We build upon user context to ensure privacy, as Steinfeld [43] noted that there is still potential for encouraging users to become more aware and informed concerning personal online data and their processing. His study advices on accessible and comprehensible information, which makes users understand the principles of their engagement with IoT applications and what they can achieve to affect the way information about them is handled.

A solution-oriented and adaptable approach to CPS development, as proposed in the following, could help to guide developers and users to engage in privacy management. Design Science-based approaches meet both requirements. Consequently, we frame the methodological integration of SDT and its instruments by Design Science. In the following, we introduce the Design Science concept and its operationalization, meeting the requirement of enabling situation-sensitive solutions, and exemplifying each step for a smart healthcare use case. Finally, we put the requirements for user-centric development derived in Section 2 in the context of valid SDT instruments for each of its dimensions.

4.1. Framing SDT-Based Development

Design Science has attracted development attention for the last decade [13,44]. Its dual while iterative nature with respect to design artifacts and design theory equally supports practical development and theory advancement. The Relevance Cycle (Figure 2) connects the environment of the maker (project) with the core development activities. The Rigor Cycle relates these activities to a knowledge base, informing the project. The Design Cycle iterates between the core development activities (building and evaluating artifacts).

In the field of home healthcare [44], taking into account privacy management, the 'people' dimension concerns all stakeholders engaged in domain-specific privacy management, such as clients of IoT systems, providers of CPS services, and producers of smart healthcare appliances. They operate in certain roles and are organized in a network for configuring and operating such a CPS. The technical systems range from simple sensors and actuators to digital twins adapting and synchronizing IoT devices at runtime to meet client demands. The opportunity for smart home healthcare is predictive analysis of behavior according to the functional needs and capabilities, taking into account privacy requirements. Design Cycles allow to focus on particular features of privacy management to meet specific requirements, e.g., anonymizing personal data when IoT device usage data are transmitted to the service provider for maintenance. The knowledge base captures all privacy requirements and their operational implementation, and thus, represents a coherent compilation of results in privacy management of developed solutions in the field of home healthcare.

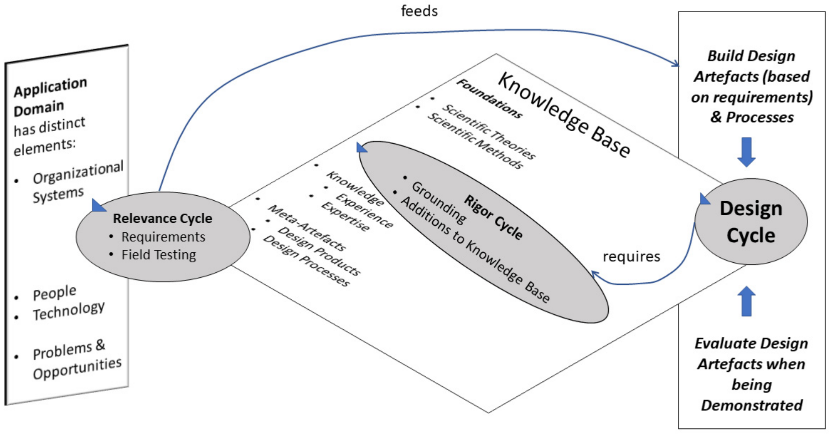

Figure 2. Design cycles embodied in pragmatic and methodological context (according to [13]).

The original framework has been operationalized by Peffers et al. [45], allowing us to frame privacy management development as shown in Figure 3. The depicted five steps correspond to those before the development process is communicated. The development process being communicated has not been included in the figure, in order to focus on the relevant part of embodying SDT into the design-driven development process.

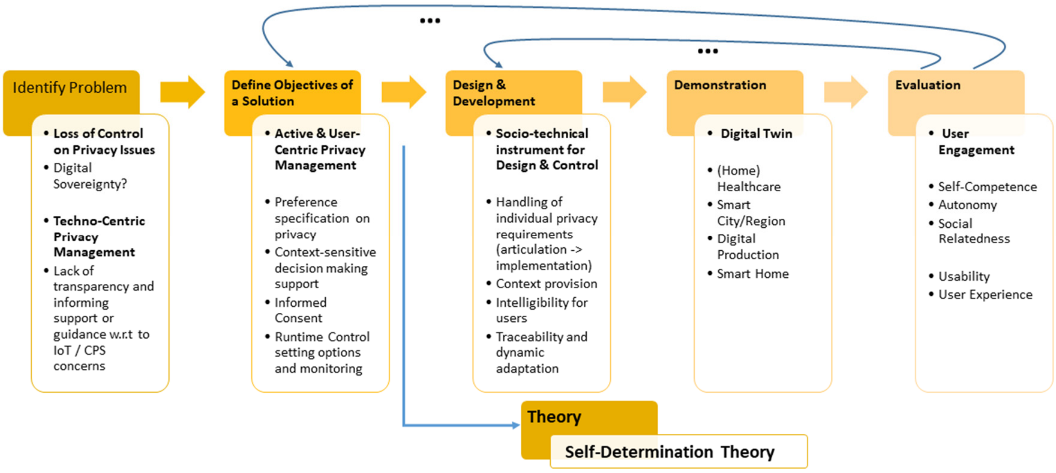
•••
•••
Identify Problem
Loss of Control on Privacy Issues
Digital Sovereignty?
Techno-Centric Privacy Management
Lack of transparency and informing support or guidance w.r.t to IoT / CPS concerns
Define Objectives of a Solution
Active & User-Centric Privacy Management
Preference specification on privacy
Context-sensitive decision making support
Informed Consent
Runtime Control setting options and monitoring
Design & Development
Socio-technical instrument for Design & Control
Handling of individual privacy requirements (articulation -> implementation)
Context provision
Intelligibility for users
Traceability and dynamic adaptation
Demonstration
Digital Twin
(Home) Healthcare
Smart City/Region
Digital Production
Smart Home
Evaluation
User Engagement
Self-Competence
Autonomy
Social Relatedness
Usability
User Experience
Theory
Self-Determination Theory

Figure 3. User-centric privacy management development based on Pfeffer et al.'s [45] operationalization of Design Science-based development.

The findings of Section 2 on privacy management not only motivate the need for engaging users in privacy management, but also defines and recognizes the requirements when designing the artefact. They correspond to the user's needs on transparency with respect to privacy data and inferences to provide informed privacy consent, and corresponding features to identify and specify privacy needs. They enable to embody contexts on privacy issues for informed decision-making when setting privacy options, and features to monitor system behavior with respect to preserving privacy. We detail each step in the subsequent section.

4.2. SDT-Informed Development Steps

In the following, we describe the operational development steps as proposed by Peffers et al. [45]. We give a general description and exemplify each step for a use case scenario, namely smart healthcare. Smart home healthcare deals with the use of IoT systems or CPS in home environments for real-time monitoring of users' health status and high connectivity of devices and experts. These systems aim for dynamically creating relations between social, professional, and health-care networks and their members while maintaining personal privacy [46]. Studies on the need for individuals' control over personal health information emphasize that health information should be kept confidential for various stakeholders, e.g., device operators. However, development effort for users of smart home healthcare requires skills to make users understand the capabilities of privacy management, thus establishing privacy management as an essential development task.

It is likely that users share their individual medical records with doctors and therapists, while they are reluctant to transmit those data to mediocre institutions. It seems 'that people's willingness to share information is not only motivated by social intimacy to the recipient but also by the competence of the recipient' [46]. Hence, the recipient's identity is a strong mediator of privacy preferences and represents essential contextual information. In addition, 'disclosure settings of health information in smart home healthcare must make room for adapting to the changes in the user's situation' [46]. Princi et al. [9] found 'that, prior to their decision, individuals weigh perceived risks and anticipated benefits of information disclosure' in the context of IoT healthcare technology. In summary, the development process of a smart healthcare lacks user engagement due to the user perceived risks outweighing the benefits of sharing data.

According to Peffers et al. [45], a development process in the context of privacy management needs to comprise the following steps: problem identification, definition of objectives of a solution, design and development, and demonstration evaluation.

Problem identification: the authors of [45] describe the definition of "the specific research problem" and the justification of "the value of a solution" as the first step in a design science research process. Researchers need to know "the state of the problem" to find appropriate solutions [45].

When users experience an increased loss of control on privacy issues and thus lack of digital sovereignty, the techno-centric approaches to privacy management are perceived as difficult to grasp by human users due to lack of system transparency. Hence, consent to privacy management activities is not given on techno-centric information or guidance, in particular, in the context of IoT and CPSs. Studies identified a lack of engagement in privacy management of private users [7,8]. This lack of engagement justifies potential SDT contributions along design cycles and embodies SDT as kernel theory into the Design Science-based development process.

Both misconceptions and self-education that is perceived by users as unhelpful in making informed decisions on privacy concerns are likely to lead to a lack of engagement and autonomy. In the studies analyzed in Section 2, all dimensions of self-determination have indirectly been addressed in the context of user roles and their activities in overcoming perceived misconceptions and technic-centricity. In order to overcome these hindrances in user engagement, and as a justification of a solution, users should be able to decide in an autonomous way based on transparent options with what or to whom they share data. Informed decision-making, and, finally, consent, is based on education and competence; thus, addressing their perception of their own competence, and relatedness to other users, either directly or via the CPS provider, is necessary

In the context of the smart healthcare case, the problem can be manifested through the lack of familiarity with IoT devices and their connectivity, resulting in a corresponding CPS. When they perceive a low level of individual competence, they do not engage in healthcare technology adoption, as they rely on others to configure and adapt CPS technologies to their needs. Such behavior influences privacy management, which in turn influences their autonomy, e.g., when devices share personal data. Social relatedness for sharing their perception could reduce the reluctance of adoption, in case the peer group is educated and relies on informed decision-making, or offers privacy management services in a supportive way.

Definition of Objectives of a Solution. After analyzing the problem in detail, feasible requirements or "objectives of a solution" must be defined. "Resources required for this include knowledge of the state of problems and current salutation, in any, and their efficacy" [45].

As mentioned in Section 3, the activation of users to participate in privacy management activities needs to be based on human-centric articulation and specification of individual requirements and preferences with respect to privacy. Any decision-making activity should be supported by situation context. It can lead to informed consent based on contextualized options. It allows users to (re)gain control and finally, monitor system behavior.

The authors of [12] examined "how information control can be enhanced." In the context of cloud storage services, they identified that psychological needs defined in SDT influence "the intention to adopt" such services. The study shows that "when individuals feel self-expressive, competent, supported, and secure, it builds the belief that they are able to control their personal information" [12]. Hence, the findings indicate the importance of SDT when aiming to foster user engagement with new systems [12].

Furthermore, the development process of a privacy management system should include the SDT perspective (see Section 3). In terms of SDT, a central objective of a private management system should be the satisfaction of the basic needs of the users when aiming to foster engagement and self-determined use. They lay ground to overcome recently addressed deficiencies in online privacy literacy. Mazur [47] suggests 'to facilitate a privacy deliberation process in which individuals become agents of social change that could lead to conditions of positive privacy and informational self-determination' (p. 258). The concerned knowledge and skills in his multi-dimensional model of online privacy literacy challenge developers and users. Developers need to provide factual privacy knowledge-sharing features, enabling users to reflect on privacy protection to finally 'protect themselves against some horizontal and vertical privacy intrusions' [47]. In case of home healthcare, the permission to access user data could be made transparent, in order to show the functional relations of services and their providers, and offer points of user intervention and control.

We took these competence-related inputs into account when formulating the entries of the table. In Table 1, we relate each SDT-addressed user need to the user-centric privacy management requirements derived from existing research in Section 2. On the basis of the summarized issues in Section 2, we have condensed the requirements for artefact design. The table reveals how they can be related to the basic needs addressed by the kernel theory in terms of design options or system features.

Design and Development means to "create the artifact. [. . .] This activity includes determining the artifact's desired functionality and its architecture and then creating the actual artifact" [45]. Any artifact in user-centric privacy management should be able to capture the articulated privacy requirements and guide design and technology adaptation. The context of the application should be easily recognized to support informed decision-making on the privacy management options.

The artefact itself is considered a socio-technical instrument for privacy management in terms of designing and controlling CPS technologies. It comprises physical and digital components as well as material to enable user autonomy and social relatedness. For smart healthcare, the physical components are sensors and other IoT systems that are at least connected by digital elements, in order to enable integrated CPS user access, privacy monitoring, and control.

Table 1. Design proposals for SDT dimensions, referring to the design of technology features relatedness.

SDT-Addressed User Needs Privacy Management Requirement	*Competence*	*Autonomy*	*Relatedness*
Transparency on data level and inferences to provide informed consent	Users are able due to intelligible access options to recognize which privacy-relevant data are collected and processed to acknowledge sharing those data. Users are able to articulate need for (additional) capacity building to provide informed consent.	It is transparent to each user which entity generates and processes privacy-relevant data and how generation and processing can be influenced, and therefore each user has the choice to intervene in providing consent.	Users perceive respect when having access to this information for providing informed consent.
Preference specification features on privacy	Users feel qualified to express their privacy preferences to influence system behavior.	Users have the access rights to edit their preferences on sharing privacy-relevant information.	Users perceive recognition of their needs when having the opportunity to provide their privacy preferences for system adaptation.
Context information for informed decision-making	The provided context information brings users into the position to make informed decisions.	Users can decide whether to utilize context information for informed decision-making.	Users can share context information with others for informed decision-making.
Privacy options setting and monitoring features throughout runtime	Users have the ability to control system behavior by setting privacy parameters at runtime and monitoring the system behavior.	Users decide when and how to monitor the implementation of their individual privacy requirements, and when and how to modify it.	Users perceive their privacy demands are taken seriously, because they can set privacy options dynamically, and monitor their implementation.

For each of the SDT dimensions, smart healthcare design proposals could include specific features. User competences could be addressed from a capacity development perspective and include educational material [48]. They could also be addressed by default options for connecting IoT components that need to be acknowledged by users such as calling the ambulance in case of a medical emergency indicated by sensor data. Relatedness could target social contacts when sharing sensitive private health conditions with persons from a peer network.

Demonstration. This step aims to demonstrate “the use of the artifact to solve one or more instances of the problem” through appropriate activities such as simulations, case studies, or experimentations [45]. In case of CPS development, demonstration should be enabled via Digital Twins as they allow interactive validation at runtime, once they are based on an executable IoT system and CPS model [49]. The entire functionality should be mapped to run realistic application cases and control CPS behavior at runtime. Such types of demonstrations address competencies of users, as model-based execution allows to simulate CPS behavior before physical components are activated with minimal prior knowledge on CSP. Because individual designs can be developed, user autonomy plays a crucial role. Finally, as the demonstrator can be shared with others, social relatedness can play a motivational role at that stage of development.

Evaluation. This step aims to find out “how well the artifact supports a solution of the problem.” Depending on the problem and the artifact, researchers need to choose appropriate evaluation methods or analysis techniques (e.g., surveys, client feedback, or simulations). Depending on the results of the evaluation, “the researchers can decide whether to iterate back to activity 3 [Design and Development] to improve the effectiveness of the artifact or to continue on to communication and leave further improvement to subsequent projects" [45].

Because we defined the satisfaction of users' basic needs as an objective for supporting the engagement in the designed privacy management system, we need to use SDT-specific instruments for the evaluation. The authors of [12] developed an SDT-informed questionnaire in the context of cloud storage with measurement items concerning Technology-based Assurance, Institution-based Assurance, Perceived Autonomy, Perceived Competence, Perceived Relatedness, Perceived Information Control, Perceived Benefits, and Intention to use. We suggest developing an artifact-specific questionnaire guided through the items by Li et al. [12]. Following the Design Science approach, the artifact needs to be adapted based on the evaluation results by iterating back to step III (Design and Development).

Evaluation refers to the perceived competence and autonomy given by the transparency on the data level and inferences for users to achieve their informed consent. It contradicts preference specification on privacy as an inherent utility function of IoT applications, and the availability of context information to support decision-making. The collective control of privacy option settings and monitoring throughout runtime brings into play social relatedness, because users can share their strategies and adopt novel ones. User experience and usability evaluation methods provide means to check user-perceived values.

The evaluation should reveal whether Li et al.'s results can be confirmed for further developments. "Of the three psychological need satisfaction variables, perceived autonomy had the strongest impact in the model, followed by perceived relatedness. Perceived competence had impact on perceived information control, but not on perceived benefit" [12]. For healthcare, these findings could mean that effective IoT playground training enables more active user participation in configuring IoT settings. Increased user involvement could lead to higher perception of individual autonomy that could be shared with others, or could serve as a model for service providers. These relations could trigger a spiral development, intensifying user engagement.

4.3. Appropriation of SDT-Instruments in Development Context

As mentioned above, overcoming misconceptions and technic-centricity by means of SDT can be addressed by the identified requirements from the shift from technic- to user-centricity. This shift can help to adjust user misconceptions, and increase user engagement. The appropriation of Li's methodological developments can be supported, as shown in Figure 4. Similar to the adoption of cloud storage services, the three psychological needs have to be fulfilled for adopting privacy management features or services. The requirements on privacy management (identified and summarized in Section 2) on human-centric technology development serve as a baseline, when users should become intrinsically motivated and engage in privacy protection. Similar to cloud storage service adoption, it can be assumed that when motivating users to engage in privacy management activities, information assurance matters, as it fulfills the basic psychological needs of individuals. This induces support of choice, initiation, and understanding (being characteristic for perceived autonomy), rather than prescriptive and normative procedures to meet privacy objectives.

We can further follow Li et al.'s [12] detailing of information assurance: (i) Technology-based assurance 'refers to the technological safeguards such as encryption, authentication, firewall, third-party certification, and feedback mechanisms so that the IT application is deemed trustworthy' ([12], p. 115), and (ii) Institution-based assurance which 'refers to the interventions that an organization initiates to assure users that efforts have been devoted to protecting their personal information' ([12], p. 115)—see Figure 4. Both types of information assurance play a crucial role in privacy management per se, recognizing the socio-technical nature of CPS.

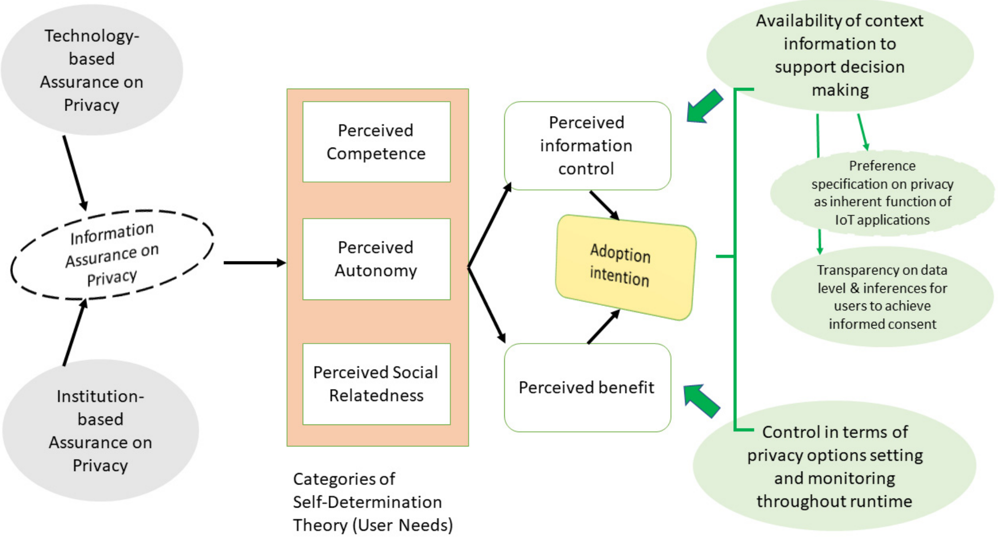
Technology-based Assurance on Privacy
Information Assurance on Privacy
Institution-based Assurance on Privacy
Perceived Competence
Perceived Autonomy
Perceived Social Relatedness
Categories of Self-Determination Theory (User Needs)
Perceived information control
Adoption intention
Perceived benefit
Availability of context information to support decision making
Preference specification on privacy as inherent function of IoT applications
Transparency on data level & inferences for users to achieve informed consent
Control in terms of privacy options setting and monitoring throughout runtime

Figure 4. Adoption intention according to Li et al. [12], in relation to the identified requirements for user-centric privacy management (right side).

Because privacy concerns have been addressed by Li et al. [12] in the context of cloud service provision and utilization, it can be assumed in the context of CPS privacy concerns that SDT needs satisfaction influences the perceived benefit of privacy management services. Depending on their perceived competence, users are able to utilize privacy options to meet their respective requirements and monitor system behavior. According to SDT, users should perceive individual autonomy in terms of having the choice to select the use of privacy management features. The perceived relatedness refers to the users' impression that their privacy concerns are taken seriously by the developers or providers of the services, and individual privacy requirements can be met and shared with others by using those features.

SDT needs satisfaction could influence the perceived information control on privacy management due to the provision of relevant context information, also in line with Li et al. [12]. When privacy management services are used for informed decision-making, users likely perceive themselves competent—they make the right decision for them on relevant privacy concerns. If they have the choice to utilize provided context information for informed individual decision-making, autonomy can be addressed in a positive way. Finally, when users experience transparency on privacy handling by a system and feel to be in control when utilizing privacy management services, they will perceive a high degree of relatedness.

In addition to the suggested appropriation of the constructs elaborated by Li et al. [12], from the list of SDT instruments available at the SDT website (https://selfdeterminationtheory.org/questionnaires/ (accessed on 2 December 2021)), we consider the Basic Psychological Need Satisfaction and Frustration Scales (BPNSFS) relevant to evaluating privacy management features along Design Science cycles (see also Figure 3). For instance, addressing the three user needs 'suggests that these must be ongoingly satisfied for people to maintain optimal performance and well-being'. Satisfying privacy requirements is considered relevant for work and life balance. Because the BPNSFS' General Scale also refers to frustration, it completes the perception of privacy management features in user-centric domains such as CPS applications providing home healthcare services. Thereby, users can be asked whether they feel a sense of choice and freedom in the course of CPS configuration and dynamic adaptation with respect to protect their privacy. They can also be asked whether most of the actions they set they need to be achieved to meet their privacy objectives. The feeling of care by other people may either refer to respected privacy settings by providers or to sharing experience with other users when implementing their individual privacy requirements. With respect to their perceived competence, their judgment on their capability can be made transparent, as well as their confidence to accomplish more challenging privacy protection tasks.

5. Conclusions

Recognizing the propagation of Cyber-Physical Systems (CPS) and Internet-of-Things (IoT) applications into everyday life and societal systems changes user behavior and capabilities. The more that users come into the position to decide in which way advanced technologies are adopted to their individual needs, the more active is the role they play along adoption. Privacy concerns occur once personal data are shared, and digital sovereignty needs to be perceived as an active asset. When addressing the user's perception of competent engagement in privacy management and monitoring of privacy-relevant CPS connectivity, Self-Determination Theory (SDT) and its established instruments can significantly facilitate user-centric design and user control.

We could demonstrate the conceptual and practical relevance of SDT when aiming to put user-centric privacy management into practice. In the context of CPS, the autonomy of users in terms of information assurance is a design issue, while privacy concerns also strongly focus on competence due to the complexity of CPS and related development and adaption issues. Privacy needs require specification and implementation support based on transparent data exchanges. Active monitoring enhances user autonomy from an operational perspective. Both the specification of individual privacy requirements and their controlled implementation influence the perceived social relatedness of users.

Hence, informing privacy management research and development by SDT through Design Science has a direct impact on (i) the identification of requirements for design input for artefacts that address the motivation of persons to engage in privacy management; this thus includes social elements that (ii) can be evaluated by established means stemming from the rich SDT knowledge base. Moreover, (iii) the focus of development can be determined by elaborating step-by-step the implementation of design options or requirements, depending on available demonstrator capabilities. The overall result is a fine-grained development procedure, explicitly taking into account social concerns in socio-technical developments.

Our future research will focus on implementing the proposed methodological approach. We expect to be confronted with addressing a trade-off between utility and privacy, as, e.g., indicated by Asiskis et al. [50]. Although the primary interest of CPS or IoT providers is to ensure some utility function for users in their application context and task-specific requirements, any generation of user-specific information might lead to privacy management activities. Although there are several techniques that scan and process user-generated data to ensure privacy, parameterizations of privacy settings need to be investigated to regulate a possible trade-off between maximizing privacy and minimizing utility and vice versa. To that respect, we expect design cycles to facilitate respective adjustments. They include evaluation of data generation and sharing approaches with respect to informational self-determination. Thereby, the artefact could be enriched by features of a meta-assistant to implement security and privacy concerns by regulating CPS elements in connection with user context [51]. Such an enrichment would not only help individual users but also organizations to take care of collected privacy data and their management. Context detection and device regulation could be supported by AI-algorithms taking into account adjusted ethical guidelines.

Author Contributions: All parts, including conceptualization, methodology, investigation, writing have been provided by both authors. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding. The authors appreciate the Applied Science Grant Support by the JKU Business School.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We acknowledge administrative and technical support by Stefan Oppl and Ines Golubovic. "Open Access Funding by the University of Linz".

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Banafa, A. Three Major Challenges Facing IoT, IEEE IoT Newsletter. 2017. Available online: https://iot.ieee.org/newsletter/march2017/three-major-challenges-facing-iot.html (accessed on 26 October 2021).
2. Dhotre, P.S.; Olesen, H.; Khajuria, S. User privacy and empowerment: Trends, challenges, and opportunities. In *Intelligent Computing and Information and Communication*; Advances in Intelligent Systems and Computing; Bhalla, S., Bhateja, V., Chandavale, A., Hiwale, A., Satapathy, S., Eds.; Springer: Singapore, 2018; Volume 673, pp. 291–304. [CrossRef]
3. Laurent, M.; Leneutre, J.; Chabridon, S.; Laaouane, I. Authenticated and privacy-preserving consent management in the Internet of Things. *Proc. Comput. Sci.* **2019**, *151*, 256–263. [CrossRef]
4. Hengstschläger, J.; Leeb, D. *Grundrechte*; Manz Publishing House: Víenna, Austria, 2012.
5. Friedewald, M. A new concept for privacy in the light of emerging sciences and technologies. *TATuP-Z. Tech. Theor. Prax.* **2010**, *19*, 71–74. [CrossRef]
6. Poletti, D. IoT and Privacy. In *Privacy and Data Protection in Software Services*; Senigaglia, R., Orti, C., Bernes, A., Eds.; Springer: Singapore, 2022; pp. 185–275.
7. Flinn, S.; Lumsden, J. User Perceptions of Privacy and Security on the Web, 2005, In PST. Available online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.60.9160&rep=rep1&type=pdf (accessed on 26 October 2021).
8. Janssen, H.; Cobbe, J.; Singh, J. Personal Information Management Systems: A User-Centric Privacy Utopia? *Internet Policy Rev.* **2020**, *9*, 1–25. [CrossRef]
9. Princi, E.; Krämer, N.C. Out of control–privacy calculus and the effect of perceived control and moral considerations on the usage of IoT healthcare devices. *Front. Psychol.* **2020**, *11*, 582054. [CrossRef] [PubMed]
10. Ryan, R.M.; Deci, E.L. Self-determination theory and the facilitation of intrinsic motivation, social development, and well-being. *Am. Psychol.* **2000**, *55*, 68–78. [CrossRef]
11. Ryan, R.M.; Deci, E.L. Intrinsic and extrinsic motivation from a self-determination theory perspective: Definitions, theory, practices, and future directions. *Contemp. Educ. Psychol.* **2020**, *61*, 101860. [CrossRef]
12. Li, Y.; Chang, K.C.; Wang, J. Self-determination and perceived information control in cloud storage service. *J. Comput. Inf. Syst.* **2020**, *60*, 113–123. [CrossRef]
13. Hevner, A. A Three Cycle View of Design Science Research. *Scand. J. Inf. Syst.* **2007**, *19*, 87–92.
14. Almutairi, M.M.; Abi Sen, A.A.; Yamin, M. Survey of PIR Approach and its Techniques for Preserving Privacy in IoT. In Proceedings of the 2021 8th International Conference on Computing for Sustainable Global Development (INDIACom), New Delhi, India, 17–19 March 2021; pp. 417–421.
15. Ziegeldorf, J.H.; Morchon, O.G.; Wehrle, K. Privacy in the Internet of Things: Threats and challenges. *Secur. Commun. Netw.* **2014**, *7*, 2728–2742. [CrossRef]
16. Skarmeta, A.; Hernández-Ramos, J.L.; Martinez, J.A. User-centric privacy. In *Internet of Things Security and Data Protection*; Springer: Cham, Switzerland, 2019; pp. 191–209.
17. Kounoudes, A.D.; Kapitsaki, G.M. A mapping of IoT user-centric privacy preserving approaches to the GDPR. *Internet Things* **2020**, *11*, 100179. [CrossRef]
18. Wachter, S. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. *Comput. Law Secur. Rev.* **2018**, *34*, 436–449. [CrossRef]
19. Ayed, G.B. *Architecting User-Centric Privacy-as-a-Set-of-Services: Digital Identity-Related Privacy Framework*; Springer Theses; Springer: Cham, Switzerland, 2014. [CrossRef]
20. Tesfay, W.B.; Nastouli, D.; Stamatiou, Y.C.; Serna, J.M. pQUANT: A User-Centered Privacy Risk Analysis Framework. In *International Conference on Risks and Security of Internet and Systems*; Springer: Cham, Switzerland, 2019; pp. 3–16.
21. Feth, D.; Maier, A.; Polst, S. A user-centered model for usable security and privacy. In *International Conference on Human Aspects of Information Security, Privacy, and Trust*; Springer: Cham, Switzerland, 2017; pp. 74–89.
22. Marky, K.; Voit, A.; Stöver, A.; Kunze, K.; Schröder, S.; Mühlhäuser, M. I Don't Know How to Protect Myself: Understanding Privacy Perceptions Resulting from the Presence of Bystanders in Smart Environments. In *NordiCHI '20: Proceedings of the 11th Nordic Conference on Human-Computer Interaction: Shaping Experiences, Shaping Society, Tallinn, Estonia, 25–29 October 2020*; Association for Computing Machinery: New York, NY, USA, 2020; pp. 1–11.
23. Knijnenburg, B.P.; Kobsa, A. Taking control of household IoT device privacy. In *CCC Sociotechnical Cybersecurity Workshop*; 2016. Available online: https://www.ics.uci.edu/~{}kobsa/papers/2016-CCC-Kobsa.pdf (accessed on 26 October 2021).
24. Bracamonte, V.; Tesfay, W.B.; Kiyomoto, S. Towards Exploring User Perception of a Privacy Sensitive Information Detection Tool. In Proceedings of the 7th International Conference on Information Systems Security and Privacy (ICISSP 2021), Online, 11–13 February 2021; Scitepress: Setúbal, Portugal, 2021; pp. 628–634. [CrossRef]

25. Pape, S.; Harborth, D.; Kröger, J.L. Privacy Concerns Go Hand in Hand With Lack of Knowledge: The Case of the German Corona-Warn-Wpp. Proceedings of IFIP International Conference on ICT Systems Security and Privacy Protection, SEC 2021, Oslo, Sweden, 22–24 June 2021; Jøsang, A., Futcher, L., Hagen, J., Eds.; Springer: Cham, Switzerland, 2021. [CrossRef]
26. Padyab, A.; Kävrestad, J. Perceived Privacy Problems within Digital Contact Tracing: A Study Among Swedish Citizens. In *ICT Systems Security and Privacy Protection, Proceedings of IFIP International Conference on ICT Systems Security and Privacy Protection, SEC 2021, Oslo, Norway, 22–24 June 2021*; Jøsang, A., Futcher, L., Hagen, J., Eds.; Springer: Cham, Switzerland, 2021; Volume 625, pp. 270–283. [CrossRef]
27. Shadbolt, N.; O'Hara, K.; De Roure, D.; Hall, W. Privacy, trust and ethical issues. In *The Theory and Practice of Social Machines. Lecture Notes in Social Networks*; Springer International Publishing: Cham, Switzerland, 2019; pp. 149–200. [CrossRef]
28. Michael, J.; Koschmider, A.; Mannhardt, F. *Process Mining System Design for IoT, CAiSE Forum*; LNBIP 350; Baracaldo, N., Rum, B., Cappiello, C., Ruiz, M., Eds.; Springer: Cham, Switzerland, 2019; pp. 194–206. [CrossRef]
29. Stöver, A.; Kretschmer, F.; Cornel, C.; Marky, K. Work in progress: How I met my privacy assistant—A user-centric workshop. In *Mensch und Computer 2020—Workshopband*; Hansen, C., Nürnberger, A., Preim, B., Eds.; Gesellschaft für Informatik e.V.: Bonn, Germany, 2020. [CrossRef]
30. Vansteenkiste, M.; Niemiec, C.P.; Soenens, B. The development of the five mini-theories of self-determination theory: An historical overview, emerging trends, and future directions. In *The Decade Ahead: Theoretical Perspectives on Motivation and Achievement*; Emerald Group Publishing Limited: Bingley, UK, 2010.
31. Ryan, R.M.; Deci, E.L. Intrinsic and Extrinsic Motivations: Classic Definitions and New Directions. *Contemp. Educ. Psychol.* **2000**, *25*, 54–67. [CrossRef]
32. Deci, E.L.; Ryan, R. *Intrinsic Motivation and Self-Determination in Human Behavior*; Plenum: New York, NY, USA, 1985.
33. Ryan, R.M.; Deci, E.L. *Self-Determination Theory: Basic Psychological Needs in Motivation, Development, and Wellness*; Guilford Publications: New York, NY, USA, 2017.
34. Taylor, G.; Jungert, T.; Mageau, G.A.; Schattke, K.; Dedic, H.; Rosenfield, S.; Koestner, R. A self-determination theory approach to predicting school achievement over time: The unique role of intrinsic motivation. *Contemp. Educ. Psychol.* **2014**, *39*, 342–358. [CrossRef]
35. Deci, E.L.; Ryan, R.M. The support of autonomy and the control of behavior. *J. Personal. Soc. Psychol.* **1987**, *53*, 1024. [CrossRef]
36. Deci, E.L.; Eghrari, H.; Patrick, B.C.; Leone, D.R. Facilitating internalization: The self-determination theory perspective. *J. Personal.* **1994**, *62*, 119–142. [CrossRef]
37. Moller, A.C.; Deci, E.L.; Ryan, R.M. Choice and ego-depletion: The moderating role of autonomy. *Personal. Soc. Psychol. Bull.* **2006**, *32*, 1024–1036. [CrossRef]
38. Chen, B.; Vansteenkiste, M.; Beyers, W.; Boone, L.; Deci, E.L.; Van der Kaap-Deeder, J.; Duriez, B.; Lens, W.; Matos, L.; Mouratidis, A. Basic psychological need satisfaction, need frustration, and need strength across four cultures. *Motiv. Emot.* **2015**, *39*, 216–236. [CrossRef]
39. Deci, E.L.; Ryan, R.M. Overview of self-determination theory: An organismic dialectical perspective. *Handb. Self-Determ. Res.* **2002**, *2*, 3–33.
40. Ryan, R.M.; Deci, E.L. The darker and brighter sides of human existence: Basic psychological needs as a unifying concept. *Psychol. Inq.* **2000**, *11*, 319–338. [CrossRef]
41. Ryan, R.M.; Mims, V.; Koestner, R. Relation of reward contingency and interpersonal context to intrinsic motivation: A review and test using cognitive evaluation theory. *J. Personal. Soc. Psychol.* **1983**, *45*, 736. [CrossRef]
42. Liu, Y. From data flows to privacy issues: A user-centric semantic model for representing and discovering privacy issues. In Proceedings of the 53rd Hawaii International Conference on System Sciences, Honolulu, HI, USA, 7–10 January 2020; University of Hawaii: Honolulu, HI, USA. Available online: http://hdl.handle.net/10125/64541 (accessed on 1 November 2021).
43. Steinfeld, N. "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Comput. Hum. Behav.* **2016**, *55*, 992–1000. [CrossRef]
44. Mohanty, S.P. Healthcare cyber-physical system is more important than before. *IEEE Consum. Electron. Mag.* **2020**, *9*, 6–7. [CrossRef]
45. Peffers, K.; Tuunanen, T.; Rothenberger, M.A.; Chatterjee, S. A Design Science Research Methodology for Information Systems Research. *J. Manag. Inf. Syst.* **2007**, *24*, 45–77. [CrossRef]
46. Rashid, U.; Schmidtke, H.; Woo, W. Managing disclosure of personal health information in smart home healthcare. In *International Conference on Universal Access in Human-Computer Interaction*; Springer: Berlin/Heidelberg, Germany, 2007; pp. 188–197.
47. Masur, P.K. How online privacy literacy supports self-data protection and self-determination in the age of information. *Media Commun.* **2020**, *8*, 258–269. [CrossRef]
48. Stary, C.; Kaar, C. Design-Integrated IoT Capacity Building using Tangible Building Blocks. In Proceedings of the 2020 IEEE 20th International Conference on Advanced Learning Technologies (ICALT), Tartu, Estonia, 6–9 July 2020; pp. 185–187.
49. Stary, C.; Kaar, C.; Jahn, M. Featuring dual learning experiences in tangible CPS education: A synchronized internet-of-things–digital-twin system. In *Companion of the 2021 ACM SIGCHI Symposium on Engineering Interactive Computing Systems*; ACM: New York, NY, USA, 2021; pp. 56–62.

50. Asikis, T.; Pournaras, E. Optimization of privacy-utility trade-offs under informational self-determination. *Future Gener. Comput. Syst.* **2020**, *109*, 488–499. [CrossRef]
51. Ruff, C.; Horch, A.; Benthien, B.; Loh, W.; Orlowski, A. DAMA–A transparent meta-assistant for data self-determination in smart environments. In *Open Identity Summit 2021, Lecture Notes in Informatics (LNI)*; Roßnagel, H., Schunck, C.H., Mödersheim, S., Eds.; Gesellschaft für Informatik: Bonn, Germany, 2021; pp. 119–130.