On the Philosophical Foundations of Privacy: Five Theses

Mohamad Gharib, John Mylopoulos

On the Philosophical Foundations of Privacy: Five Theses

Mohamad Gharib[1,2][0000−0003−2286−2819] and John Mylopoulos[3]

[1] University of Tartu, Tartu, Estonia
[2] University of Florence, Florence, Italy
mohamad.gharib@{ut.ee,unifi.it}
[3] University of Trento, Trento, Italy
john.mylopoulos@unitn.it

Abstract. Privacy has emerged as a key concern for companies that deal with Personal Information (PI) since they need to comply with certain privacy requirements. Unfortunately, these requirements are often incomplete or inaccurate due to the vagueness of the privacy concept. This paper tries to tackle this problem, contributing to the philosophical foundations of privacy by addressing several foundational questions such as What is privacy? What makes information a PI? Is PI a property? Do we own our PI? To what extent we are entitled to protect our PI? How do we protect our PI? After answering the aforementioned questions, we characterize the privacy concept that allows providing a more precise and meaningful conceptualization of privacy requirements, which may improve dealing with them during the design of privacy-aware systems.

Keywords: Privacy · Personal Information · Philosophical Foundations · Conceptual Modeling · Requirements Engineering.

1 Introduction

Privacy has emerged as a key concern for companies that collect and manage PI since they need to comply with certain privacy requirements [1]. If such privacy requirements were captured and addressed appropriately during system design, most of the privacy concerns could be tackled. Unfortunately, privacy requirements are often inaccurate and incomplete, which is mainly due to the vagueness and complexity of the privacy concept [2]. More specifically, many requirements engineers limit the wide scope of privacy requirements to narrow perspectives (e.g., confidentiality, secrecy) [3].

Privacy is one of the few concepts that has been thoroughly studied across many disciplines for centuries, including Psychology [4], Philosophy [5,6], Sociology [7], Law [8,9,10], and Political Science [11] to mention a few. Despite this, it is still elusive and vague concept to grasp [3,12,13]. Moreover, there is no consensus on the definition of the privacy concept among these disciplines [3]. For instance, privacy has been defined as "the right to be left alone" [8], and "a state of limited access to self" as defined in [11]. Other scholars (e.g.,

[14]) defined privacy as a "control over when and by whom the various parts of us can be sensed by others". Several other scholars recognized that privacy cannot be limited to a single concept [3], and they consider integrating different conceptions (called "cluster formulations") to define privacy.

On the other hand, several researchers differentiate between what can be called *general privacy theories* [11,4,12] that considers both the *spatial* and *informational* perspectives, and *information privacy theories* that focuses mainly on the *informational* perspective [13], which is the main focus of this paper. All of this has led to confusion when dealing with privacy requirements either on the side of requirements engineers or on the side of individuals, who are expected to play an active role in specifying their privacy requirements.

In previous research [15,16], we proposed an ontology for privacy requirements that has been mined through a systematic literature review [2,17]. The ontology has been implemented, validated, and its completeness/coverage was evaluated with the help of privacy and security researchers. However, an ontology is concerned with answering questions like *what entities exist*, not *why they exist*, which can be answered relying on metaphysics that studies the very nature of an entity and explains why it exists [18].

This paper tries to tackle this problem contributing to the philosophical foundations of privacy by addressing several foundational questions related to the concept of privacy such as "What is privacy?", "What makes information a PI?", "To what extent we are entitled to protect our PI?" Answering these questions can widen our knowledge and understanding of the privacy concept allowing us to identify five key theses of privacy, which we use to characterize the privacy concept. This enables a more precise and meaningful conceptualization of privacy requirements, which may facilitate and improve dealing with them by increasing privacy awareness on the side of both requirements engineers and individuals during system design.

The rest of the paper is structured as follows; Section 2 presents a historical overview of the privacy concept. Section 3 discusses the philosophical foundation of privacy identifying five key theses of privacy, and Section 4 characterizes the privacy concept in light of the aforementioned theses. Section 5 proposes a new conceptualization of privacy. We discuss challenges and future work in Section 6, and we conclude the paper in Section 7.

2 The Concept of Privacy: A Historical Overview

The concept of "privacy" has historical origins that date back into antiquity, most notably in Aristotle's distinction between the public sphere and the private one that is associated with family and domestic life [19]. Similarly, the concept of privacy ("being private") was linked to the individuals' private properties (e.g., own house) in Roman times [6]. In fact, the Latin word "privatus" makes a legal distinction between what is "private" and what is "public" ("publicus") [20]. Hence, both of the Greeks and Romans have almost the same view concerning

privacy, which was geared more toward the sense of property, i.e., what is private should belong to an individual's property, otherwise, it is public.

According to Holvast [21], this sense continues to exist during the *Early modern period (1450-1800)* as people went to court for eavesdropping or opening and reading personal letters. The same sense still survives today with the legal recognition of the individuals' right to property [6]. In particular, it has been grounded in Law when the "privacy as a right" was born, first defined by Warren and Brandeis [8] in 1890 as the "the right to be left alone", which became central to legal interpretations and court decisions [13].

Debates concerning privacy became prominent in the second half of the twentieth century. For instance, Prosser [9], in his highly influential paper that shaped the development of the American law of tort privacy, divided the "right to privacy" into four discrete torts: 1- an intrusion upon the plaintiff's seclusion, solitude, or private affairs; 2- public disclosure of embarrassing private facts about the plaintiff; 3- publicity that placed the plaintiff in a false light in the public eye; and 4- appropriation for the defendant's advantage of the plaintiff's name or likeness. Although Prosser gave tort privacy legitimacy, he also limited its ability to adapt to the problems of the Information Age [10]. In particular, privacy has been mainly understood in a narrow sense referring to physical privacy in the home or office, etc. [7], i. e., what happened behind "closed doors" stays there. This perspective "fail short" to deal with recent privacy concerns such as the extensive collection, use, and disclosure of PI [10].

Besides Law, other disciplines have their contributions to the concept of privacy. For example, privacy has been viewed as a feeling, an emotion, a desire that supports our social interaction with others in Psychology [13]. In Philosophy, privacy was defined as "a state of limited access or isolation" [5]. Economists have sketched the essential elements of privacy based on economic value [22]. In Political Science, privacy was defined in terms of self-determination, i.e., it provides individuals and groups with preservation of autonomy [11]. In Sociology, privacy was approached from the "power and influence" perspectives between individuals, groups, and institutions within society [7].

Each of these definitions carries a set of dimensions that point to the multidimensional nature of privacy [13], which motivated expanding the view on the privacy concept to include a number of so-called *privacy interests* [23] such as control [14], confidentiality [8], self-determination [11], solitude [9], anonymity [24], secrecy [12], etc. Such interests (concepts) can be considered as dimensions of privacy [13], which contributes to the confusion while dealing with privacy.

3 The philosophical foundation of privacy

Privacy has received relatively little attention from philosophers compared to other important concepts, such as Freedom, Human rights, or Democracy [6]. Nonetheless, there are very interesting philosophical works related to privacy, and the main focus of this section is to review these works trying to contribute to our understanding of key philosophical aspects of privacy.

What privacy is: the five theses of privacy. It is natural for a complex concept like privacy to have a variety of definitions [6]. As we saw earlier, philosophers, psychologists, sociologists, economists, and legal theorists have great difficulty in reaching consensus on a definition of privacy even in their respective domains [25]. Such diversity of definitions indicates uncertainty concerning what privacy is [14], which led some scholars to even renounce the idea of providing a precise definition of privacy [3,6]. However, the core aspects of privacy can be identified by comparing the commonalities in how scholars have approached this complex concept. Reviewing the existing definitions of privacy, it can be noted that most of them agree on most of the following five key aspects:

1. Privacy is centered around an *individual*, who can claim it;
2. The *private sphere* (not necessarily physical) entitles the individual to protect only a subset of her PI;
3. An individual should have *a right* to justify her claims concerning the protection of her PI, especially, outside of her *private sphere*;
4. An individual should have a "sort" of *ownership* over her PI; and
5. An individual should be entitled to *control* the "use" of her PI.

The thesis of this paper is considering these aspects as the five theses of privacy and discussed in the rest of this section.

3.1 Thesis one: Privacy as an individual right

The conceptual relationship between privacy and the individual has received vast attention in the philosophical discussions [6,26]. We have seen that privacy was linked to individuals and their private properties since Greek and Roman times, and the relation between privacy and individuals is clear in many definitions of privacy. For example, privacy has been also considered as an essential requirement for an individual's autonomy [27,28], her freedom of choice and actions [26], and her moral worth and dignity [5] to mention a few.

According to Hongladarom [6], privacy seems to be a quintessentially individual concept, and it is seen as something that only an individual enjoys [11,6]. Therefore, the individual is central in any definition of privacy, simply because without an individual, there is no need for privacy. In such a context, one main difference between information and PI is the individual that PI is related to. Moreover, most scholars consider that PI also covers some of the individual's activities/behavior, etc. [22]. However, do we consider any information that is related to an individual, her activities, etc. as her PI? Many relatively recent studies (e.g., [24,15]) highlighted that information should allow the identification of an individual to be considered her PI, i.e., it is not sufficient to be only related to an individual but it also should "sufficiently" identify her. To this end, the main objective of this thesis is answering *whether an information item can be considered PI, and if it is, identifying the individual it is related to.*

The question now is, are we entitled to protect (e.g., control the access and use of) all of our PI? Consider for example a manager who wrote a recommendation

letter for one of his employees. Information in such a letter is surely related to the employee (an identified or identifiable natural person) as it describes some of her professional characteristics, her attitude towards work, activities she performed, etc. But why she cannot control the access and use of such information? Or even read the letter unless she was permitted by the manager who wrote it? We will elaborate on this issue while discussing the other theses of privacy.

3.2 Thesis two: Privacy as solitude in the private sphere

We have seen that an individual is essential for privacy, and we discussed when information can be considered PI. The question now, *How we can specify when an individual is entitled to protect her PI?* A good starting point could be the notion of private sphere [6,26]. As previously discussed, the sense of privacy that is related to a private sphere, separating what is private and what is public, has been grounded in Law when the "privacy as a right" was born in 1890 [8]. Although, this line is not clear as it used to be, the notion of separating what is private from what is public survived.

To understand the main purpose of such a sphere, we need to answer the question: *Why an individual needs a private sphere?* According to various researchers (e.g., [6,11]), individuals behave differently when they know they are being watched as they behave according to the wish of others rather than of their own free will [26]. Other scholars believe that such a sphere is necessary for an individual's autonomy [27,5]. Therefore, a main purpose of a private sphere is to allow an individual to maintain her autonomy and freedom of behavior by controlling when, and to what extent she can be accessed by others.

We know, by now, that a private sphere is related to an individual, and may represent a physical or a virtual area, where an individual may exist and perform her activities. What is not clear, *How can we specify such sphere?* Considering the letter example, if the employee exists and behaves within a private sphere that preserves her PI/privacy, how such letters can be written? We know that the letter contains information related to the employee's professional characteristics and activities. We also know that such a letter does (or should) not contain any information related to the employee's private life (e.g., religion, sexual orientation). Why it is ok for some PI to be used almost "freely" by others, while for other PI, it is forbidden?

Reviewing the PI included in the letter, it is easy to note that such PI describes employee's characteristics or activities that are "publicly" available or were performed, where she cannot control who has access to her PI/activities. While PI that has not been included in the letter can be considered private to the employee and she can control (or has the right to control) who has access to them. Thus, a main distinctive feature of the private sphere is the individual's right (and capability) to control who has access to it.

To this end, the private sphere can be described as any physical or virtual area, where an individual may exist (e.g., house) and/or perform activities (e.g., cellphone) and has the right and capability to control who has access to it. In this context, this privacy thesis aims at answering *whether a sphere can be considered*

private, and if it is, the individual is entitled to control access to it by various means. Note that if the individual failed to properly control the access to such sphere, no one has the right to acquire, collect or use any PI enclosed in the private sphere. We will elaborate more on this issue while discussing thesis five.

3.3 Thesis three: Privacy as property and legal right

Almost half a century ago, Thomson [29], a notable philosopher who worked on Ethics and Metaphysics, stated that *the most striking thing about the right to privacy is that nobody seems to have any very clear idea what it is.* In what follows, we will discuss the different approaches that have been followed to interpret the right to privacy, and argue on which basis privacy claims can be justified.

One of the most legalistic approaches to safeguarding privacy that has been offered to information is the notion of treating PI as a property [30,31,32]. However, this notion has lost its momentum in the early 2000s [30,31], since it mainly considers negative rights[4] whereas positive rights are also vital for PI protection and should be considered as well [33].

Other philosophers and scholars have come to doubt that there is anything distinctive about the right to privacy [34]. For instance, Thomson [29] stated that "there is no such thing as violating an individual's right to privacy by simply knowing something about him". She further argued that whatever rights to privacy a person has, such rights can be fully derived from property rights, and rights a person has over his own self [34]. In Thomson's view, privacy is a cluster of derivative rights. A similar view was adopted by Posner [22], who argued that a person's right to privacy is violated only if another, more basic, right has been violated [5].

On the other hand, several scholars have argued that there is something distinctive about the right to privacy but it cannot be captured relying only on property rights or rights over individual's herself [5,32,31,34]. In response to that, they propose to adopt a more novel paradigm. For example, Samuelson [31] suggested considering a moral rights-like approach. Other scholars debate that the law, in general, can grant individuals a protectable interest concerning their PI without grounding such interest on fundamental rights [35], personal rights [5] or even property rights [31,34,32]. Finally, several researchers argued that the propertisation of PI might be required but it is not sufficient, and regulation should be also considered [30,33].

As the principle aim of this thesis is answering the question *on which basis privacy claims can be justified?* We favor adopting the notion of a hybrid model of property and legal/regulation based rights that an individual can have, which she can employ to protect her PI. Such model justifies why some PI have been included or excluded from the letter, and why the employee cannot claim any right concerning the content of such letter since she "willingly" made such PI publicly available to others.

[4] A negative right exists unless someone acts to negate it, while a positive right is a right to be subjected to an action of another person or group

3.4 Thesis four: Privacy as ownership of PI

The concepts of ownership have been of interest throughout history, and some researchers suggest that advanced forms of ownership appeared more than 10000 years ago. In the late nineteenth century, the ownership concept was linked to the producing entity, i.e., the owner is the person who has "produced" (found and appropriated) the object [36]. Recently, Janeček [37] discussed three property-based ownership theories concerning information: 1- *first occupancy theories*, grants ownership rights to the producer of information; 2- *last occupancy theories*, grants ownership rights to those who get last to gain control of the information; and 3- *the Humean theories*, in which ownership rights are justified by common sense that is recognized by the community. Janeček stated that these theories are far from being perfect for allocating ownership concerning information since they are mostly inspired by the notion of property ownership.

Concerning the letter example, can we consider the employee as the owner since most information included in it describes activities that were performed by her (*first occupancy theory*)? Or the owner should be the manager who wrote the letter? Since the manager is the actual producer of the letter content. We may argue that the *last occupancy theory* might also apply to grant ownership to the manager since he was the last to gain control of information. Relying on the same theory, the recipient of the letter can also claim ownership. Finally, it is clear that we cannot rely on common sense to specify the owner.

To this end, relying on a pure property-based ownership right might not be adequate for specifying the owner of information. Yet, if ownership is also based on legal/regulation rights this issue might be solved [37]. In this context, and as the main objective of this thesis is answering *what "sort" of ownership an individual can have over her PI.* We believe that adopting property and legal/regulation based ownership approach, in which the individual is, usually, the owner of her PI is the best approach to solve this problem.

It is worth mentioning that providing ownership rights concerning novel "objects" is not a smooth process. For example, intellectual property represented a challenge when it was first introduced since rights in such case do not concern solely a tangible object, rather, the object is intangible [38]. Back to letter example, the employee cannot claim any property or legal/regulation-based ownership rights concerning the content of the letter as she made such information available to be used by others.

3.5 Thesis five: Privacy as control over PI

We saw that privacy is not an absence of information about us; rather it is having the capability to control our PI. The question now *Why does an individual wants to control the collection, disclosure, and usage of her PI?* The answer is quite simple, when privacy is invaded, breached or violated, it is lost, which may result in consequences of having an individual's information in "the wrong hands". Therefore, one of the most cited and notable reasons for controlling the collection, disclosure, and use of PI is concerns/risks of losing privacy (e.g.,

breaches, violations, misuse) [13]. But *How individuals, as owners, control the collection, disclosure and usage of our PI?* Massin [39] provides an extensive discussion on the metaphysics of ownership rights differentiating between the property, its possession, and the rights over it.

Although ownership of PI is not exactly as the ownership of a property as discussed earlier, the same notions can be applied to PI. To this end, we base our discussion while answering *what kind of control an individual is entitled to over the "use" of her PI*, the main objective of this thesis, on Massin's work. In short, PI is distinct from its possession and from rights over it. An individual is, usually, the original owner of her PI and holds absolute rights over it. Ownership over PI can be transferred by the owner. Similarly, rights over PI can be transferred/granted by the owner—temporarily or permanently, partly or wholly, conditionally or unconditionally, even without transferring ownership. An individual can transfer these rights in terms of permissions (e.g., possession, collect) to other legal entities. Finally, PI can be possessed and transferred/shared, yet possession of PI does not ground any right, i.e., it is possible to possess PI without having any right to use it.

4 Characterizing the privacy concept

After identifying and discussing the five theses of privacy, we can define privacy as the ability of an individual to express herself selectively to others by controlling the collection, use, share, etc. of her PI. A simplified representation of the concepts identified while discussing the five theses is shown in Fig. 1. We can identify an individual and her two spheres (e.g., private and non-private instead of public).

PI can be specialized into two sub-categories: 1- *private PI* represents any PI that has a private nature and the private sphere can be employed to protect it; and 2- *non-private PI* represents any PI that cannot be classified as a private PI. An individual has full ownership and control over her PI (private and non-private PI) unless she willingly made such PI public, thus, we can identify another category of PI that is *PI made public*. In this category, the individual does not have any ownership or right to control over PI concerning privacy as she loses them when such PI has been made public by her, i.e., *PI made public* can be collected, used, disclosed/shared without the individual permission. Despite this, it is assumed that such PI will be used in contexts compliant with the purposes for which it has been disclosed.

Concerning the collection of non-private PI, the individual should be notified about such collection and she can decide whether to allow it or not. For example, entering a supermarket or any other place, which clearly states that they are using surveillance cameras (notice) means that the individual implicitly consents (grant permission) for the collection of her non-private PI (e.g., shopping activity). However, collected PI can be used only for the purposes specified in the collection and cannot be shared without the individual's permission.

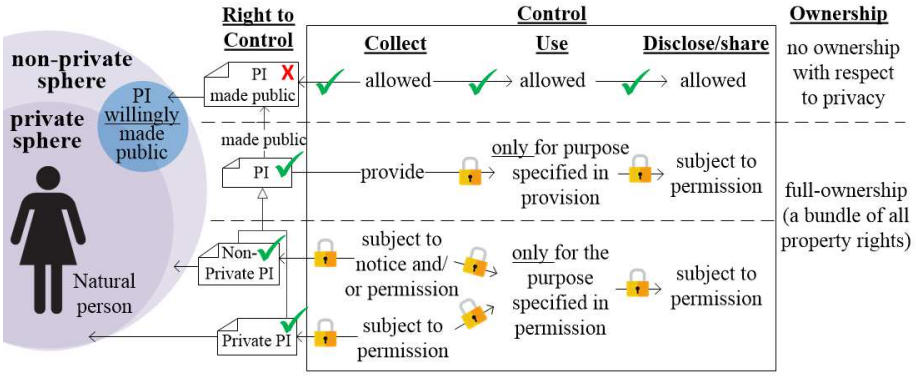

Fig. 1. An individual, her spheres, categories of PI, right to control, control and ownerships over such PI categories

As private PI are supposed to be protected within the private sphere, its collection is subject to permission. For example, various technologies exist these days for sensing/collecting the vital signs, location, and activities of elderly individuals and forward such PI to a medical authority, which allows for evaluating their health status remotely and continuously. The collection, usage, share, etc. of such PI is subject to the individual's permission.

5 Conceptualizing privacy requirements

Naturally, the concept of privacy requirement is centered on the five aforementioned privacy theses, and the main aim of this section is to crystallize the privacy requirement concept, exploring its underlying rationality by answering two questions: 1- *What are the main characteristics of privacy requirements?* How are they different from other types of requirements? and 2- *How can we qualify the quality of privacy requirements?* Then, we provide a more precise and meaningful conceptualization of privacy requirements.

5.1 The underlying rationality of privacy requirements

Privacy requirements are supposed to capture an individual's privacy needs concerning her PI. Therefore, a privacy requirement should be composed of an individual, PI she has a right to control as well as her privacy needs concerning such PI. Accordingly, any requirement that does not include any of these three elements cannot be considered a privacy requirement.

Like other types of requirements, privacy requirements should ideally be: "complete" (capture all relevant privacy needs of an individual), consistent (such that should not be conflicting), unambiguous/clear (such that a privacy requirement can be easily interpreted, i.e., preferably has only one interpretation), realistic (such that they can be actually realized), and verifiable (such that it is

known how to, and practically possible, to verify whether the system can satisfy them). Unlike most other types of requirements, privacy requirements are very context-dependent, i.e., changing the context of the application may raise new privacy concerns, which makes it very difficult to continuously satisfy them [40]. More importantly, they are hard to be clearly and unambiguously specified due to the complexity of the privacy concept [41,1].

We know, by now, the basic elements of a privacy requirement, its key characteristics that they shared or not with other types of requirements but *How can we qualify the quality of privacy requirements?* Privacy requirements should be specified by an individual in response to her concerns/risks of losing privacy as discussed in Section 3 (Thesis five: Privacy as control over PI). However, as highlighted by many scholars (e.g., [13,10,41]), individuals fail short in clearly understanding related privacy risks. In turn, they may not have the ability to specify complete, consistent, unambiguous, realistic and verifiable privacy requirements. This leads to confusion not only concerning the specified privacy requirements but also how privacy concerns can be mitigated.

Based on [41], an individual can make an informed decision concerning her privacy requirements if she knows related laws and regulations concerning privacy protection (e.g., the General Data Protection Regulation (GDPR) [42]), strategies for privacy control, and most importantly, potential privacy threats and how such threats can be dealt with. In this context, it is crucial to make individuals aware of potential privacy threats, which allow them to frame their privacy concerns, and in turn, specify their privacy requirements in a realizable way that can tackle such concerns. To elaborate on this issue, we consider an individual called Lara that is planning to use a dating App on her cellphone. Then, we will list key privacy concerns that she became aware of, and discuss how various privacy requirements, we have mined through a systematic literature review [17][5], can be specified and realized to tackle such concerns.

Lara needs to provide some PI to the App to be used for delivering the dating service, yet she might be worried (a privacy concern) that her PI might be used for purposes rather than the dating service. To mitigate such concern, she might have a *confidentiality requirement* concerning the use of her PI, which guarantee that her PI: 1- will not be disclosed to/shared with another entity without her permission (non-disclosure), 2- will only be used if it is strictly necessary for a certain purpose, and 3- will only be used for specific and legitimate purposes (Purpose of Use (PoU)). Even with the confidentiality of her PI is assured, she might consider the risk that her PI might be leaked, breached, etc. due to a wrong practice on the service provider side. To hold them accountable for such breach, an *accountability requirement* might be specified at her side. Finally, if she is no longer interested in using the App but she is worried that the service provider will not delete her PI when she uninstalls the App, she can rely on *the*

[5] In [17], privacy requirements were further specialized into more refined concepts such as confidentiality, anonymity, unlinkability, unobservability, notice, minimization, transparency, accountability, and the right to erasure/ be forgotten

right to erasure/be forgotten (a privacy requirement) to assure that her PI will not be kept by the service provider.

5.2 A new conceptualization of privacy requirements

Following Solove [3], a bottom-up approach has been adopted, which starts conceptualizing privacy requirements within particular contexts focusing on concrete practices. Additionally, we adopted the three criteria for characterizing privacy proposed by Parker [14]. In which, a characterization of privacy requirements should 1- not be overbroad or too narrow; 2- be simple and easily understandable; and 3- be applicable, i.e., allows answering key questions like whether an individual is allowed to the right of privacy, whether she has lost privacy, whether she knows that she has lost privacy, how her privacy has been lost, etc. For example, if a privacy requirement is viewed as a feeling, an emotion, or a psychological state, it would be almost impossible to deal with it concretely.

Based on the previously presented notions, a conceptual model[6] (depicted in Fig. 2) that contains key privacy concepts and relationships for dealing with privacy requirements has been developed. The concepts of the model can be broadly organized into five subcategories of concepts corresponding to the five key theses of privacy. Concerning the first thesis of privacy, we can identify the *natural person* concept that is specialized from the *legal entity* concept, which can be an individual, a company, or an organization that has legal rights and obligations. The *Information* concept can be specialized into two concepts: *PI* and *non-PI,* where the first represents any information that can be *related* to an identified or identifiable legal entity while the last represents any information that cannot be *related* to an identified or identifiable legal entity.

Concerning the second thesis, we can identify the *Sphere of Action (SoA)* concept, which represents a physical or virtual operational environment that is a part of a *domain*. A *natural person* can *perform activities* in a *SoA*. An *activity* can be a *private* or *non-private*. The first can be *described* by *private PI* and must be performed in a *private sphere*, where the *natural person* have a right and can control access to it. While the last can be *described* by *non-private PI* and can be performed in a *non-private sphere*. For the third thesis, we can identify the *superior authority* that can *set governance rules*, which can be defined as a group of policies and decision-making criteria that *determine* the *authority*, which *empowers* the *natural person* to *control* her *PI subject to the right to privacy*. Such PI covers *private* and *non-private PI* that has not been made public by the *natural person*. Concerning thesis four, we can identify the *ownership* relationship between the *natural person* and her *PI* that has not been made public by her, i.e., *PI subject to the right to privacy*. Accordingly, *PI not subject to the right to privacy* covers any *PI* that has been made public by the natural person, and she does not have *control* nor *ownership* over such *PI*.

Concerning the fifth and final privacy thesis, a *natural person* may have or can become *aware of privacy concerns*, as a response, she *specifies* her *privacy*

[6] For reasons of readability, multiplicity and other constraints have been left out

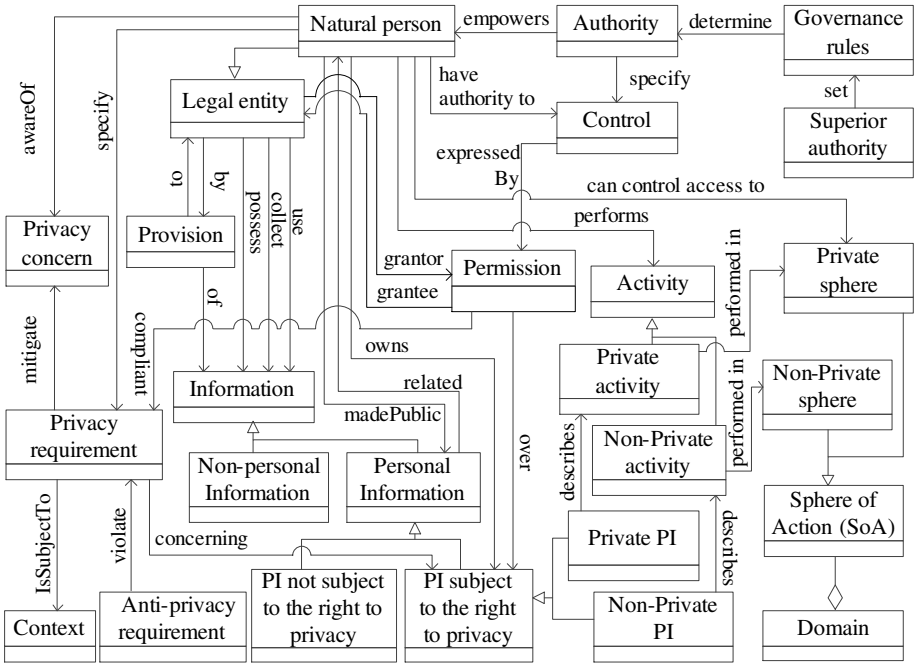

Fig. 2. The meta-model of the propose conceptual model

requirements (e.g., confidentiality, anonymity) to *mitigate* such *concerns*. A *privacy requirement* is subject to a *context* that identifies the state of affairs relevant to the *requirement*. A *privacy requirement* can be *violated* by what can be called an *anti-privacy requirement* that represents the requirement of a *legal entity* with malicious intent (e.g., misusing, breaching, spying) concerning privacy/PI.

A *natural person* have authority to *control* her *PI subject to the right to privacy*, where such *control* can be *expressed by permissions* that specify the type (e.g., possess, transfer) and the *purpose* of PI use. *Permissions* can be *granted/revoked*, initially, by the *natural person*. Granted *permissions* should be *compliant* with the *privacy requirements* that are *specified* by the *natural person concerning* her *PI subject to the right to privacy*. Finally, a *legal entity* may *possess*, *collect*, *transfer* and/or *use PI subject to the right to privacy*. However, possessing, collecting, transferring, the type and purpose of information usage is subject to having related *permissions*.

6 Challenges and Future Work

Having formulated a new conceptualization of privacy requirements, we list and discuss several significant challenges related to this track of research, which provide opportunities for future research:

A model for PI ownership: Many may agree that ownership of PI cannot be shared [39]. Yet, we have many examples, when this notion does not hold. For instance, do we own our DNA? given that we share a big portion of it with our relatives, ancestors, and offspring. Therefore, a model for PI ownership that is capable of answering this and similar questions should be developed.

Ownership of anonymized PI: It is arguable whether anonymized PI can be considered as PI. Thanks to the excessive availability of PI and profiling techniques, a small item of PI (e.g., IP address) that may identify a person can be combined with anonymized PI and violates her privacy. Thus, the relationship between a person and her anonymized PI needs to be revisited in light of the new advancement of technologies.

Collection of public PI: A deep investigation of the collection of PI that has been made public is required to better understand when such collection is "acceptable" or it can be considered as a type of invasion of privacy.

Usage of public PI: As previously mentioned, individuals may disclose some of their PI for public use with the assumption that such PI will be used in contexts compliant with the purposes for which PI has been disclosed. Analyzing whether the usage of such PI is compliant with disclosure purposes is challenging and requires concretely characterizing both contexts of usage as well as purposes of disclosure, which is on the list of future work.

7 Conclusions

Like architectural foundations that provide an underpinning for buildings, philosophical foundations for privacy provide basic concepts, relationships and assumptions that enable the definition and analysis of privacy requirements. This paper contributes to our understanding of privacy by investigating its philosophical foundations, identifying its core theses, and based on these, formulating a new conceptualization of privacy requirements. The proposed conceptualization of privacy requirements is expected to facilitate and improve dealing with privacy requirements by increasing awareness concerning such requirements on the side of requirements engineers as well as individuals who are expected to play an active role in specifying their privacy requirements.

In this paper, we provide a preliminary check for the validity of our proposed conceptualization of privacy requirements, which needs to be complemented in the future with empirical validation through controlled studies. The main aim of this track of research is proposing a well-defined privacy ontology, which when completed would constitute a great step forward in improving the quality of privacy-aware systems. Therefore, we plan to integrate the conceptual model developed in this paper into our ontology for privacy requirements that we have proposed earlier [15,16]. This will significantly improve the capability of the ontology for capturing more explicit knowledge concerning PI and, in turn, privacy requirements, which will allow a more comprehensive analysis concerning such requirements.

References

1. Gharib, M., Salnitri, M., Paja, E., Giorgini, P., Mouratidis, H., Pavlidis, M., Ruiz, J.F., Fernandez, S., Siria, A.D.: Privacy Requirements: Findings and Lessons Learned in Developing a Privacy Platform. In: the 24th International Requirements Engineering Conference, IEEE (2016) 256–265 https://doi.org/10.1109/RE.2016.13
2. Gharib, M., Giorgini, P., Mylopoulos, J.: Towards an Ontology for Privacy Requirements via a Systematic Literature Review. In: International Conference on Conceptual Modeling. Volume 10650 LNCS. (2017) 193–208 https://doi.org/10.1007/978-3-319-69904-2_16
3. Solove, D.J.: Conceptualizing privacy. California Law Review **90**(4) (2002) 87-155 https://doi.org/10.2307/3481326
4. Altman, I.: Privacy: a conceptual analysis. Environment and behavior **8**(1) (1976) 7–29
5. Schoeman, F.D.: Privacy: Philosophical Dimensions. American Philosophical Quarterly Pittsburgh, Pa **21**(3) (1984) 199–213 https://doi.org/10.2307/20014049
6. Hongladarom, S.: Philosophical Foundations of Privacy. In: A Buddhist Theory of Privacy. (2016) 9–35 https://doi.org/10.1007/978-981-10-0317-2_2
7. Waldo, J., Lin, H.S., Millett, L.I.: Engaging privacy and information technology in a digital age. National Academies Press (2007) https://doi.org/10.17226/11896
8. Warren, S.D., Brandeis, L.D.: The Right to Privacy. Harvard Law Review **4**(5) (1890) 193 https://doi.org/10.2307/1321160
9. Prosser, W.L.: Privacy. California Law Review **48** (1960) 383
10. Richards, N.M., Solove, D.J.: Prosser's privacy law: A mixed legacy. Calif. L. Rev. **98** (2010) 1887
11. Westin, A.F.: Privacy and freedom. Washington and Lee Law Review **25**(1) (1968)
12. Solove, D.J.: A Taxonomy of Privacy. University of Pennsylvania Law Review **154**(3) (2006) 477. https://doi.org/10.2307/40041279
13. Dinev, T., Xu, H., Smith, J.H., Hart, P.: Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. European Journal of Information Systems **22**(3) (2013) 295–316. https://doi.org/10.1057/ejis.2012.23
14. Parker, R.B.: A definition of privacy. Rutgers L. Rev. **27** (1973) 83–104
15. Gharib, M., Mylopoulos, J., Giorgini, P.: COPri - A Core Ontology for Privacy Requirements Engineering. In: Research Challenges in Information Science. Vol. 385, Springer (2020) 472–489. https://doi.org/10.1007/978-3-030-50316-1_28
16. Gharib, M., Giorgini, P., Mylopoulos, J.: COPri v.2 — A core ontology for privacy requirements. *Data and Knowledge Engineering*, **133**, 101888, 2021. https://doi.org/10.1016/j.datak.2021.101888
17. Gharib, M., Giorgini, P., Mylopoulos, J.: An Ontology for Privacy Requirements via a Systematic Literature Review. Journal on Data Semantics 9(4), 2020, 123-149. https://doi.org/10.1007/s13740-020-00116-5
18. Nodelman, U., Allen, C., Perry, J.: Stanford encyclopedia of philosophy. page 380, 2002. https://doi.org/10.1145/544317.544327
19. Romano, N.C., Fjermestad, J.: Privacy and Security in the Age of Electronic Customer Relationship Management. International Journal of Information Security and Privacy (IJISP) **1**(1) (2007) 65–86. https://doi.org/10.4018/jisp.2007010105
20. Richardson, J.S.: The Ownership of Roman Land: Tiberius Gracchus and the Italians. Journal of Roman Studies **70** (1980) 1–11. https://doi.org/10.2307/299552

21. Holvast, J.: History of privacy. In The History of Information Security, pp. 737-769. Elsevier Science BV, 2007. https://doi.org/10.1016/B978-044451608-4/50028-6
22. Posner, R.A.: The right of privacy. Ga. L. Rev. **12** (1977), 393
23. Milberg, S.J., Smith, H.J., Burke, S.J.: Information privacy: corporate management and national regulation. Organization science **11**(1) (2000), 35–57
24. Pfitzmann, A., Hansen, M.: A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management. Tech. University Dresden (2010) 1–98
25. Gavison, R.: Privacy and the limits of law. The Yale Law **89**(3) (1980) 421–471
26. Introna, L.D.: Privacy and the Computer: Why We Need Privacy in the Information Society. Metaphilosophy **28**(3) (jul 1997) 259–275. https://doi.org/10.1111/1467-9973.00055
27. Rossler, B.: The value of privacy. John Wiley & Sons (2018)
28. Solove, D.: Understanding Privacy. Harvard University Press (2008)
29. Thomson, J.J.: The Right to Privacy. Philosophy & Public Affairs (1975) 295–314
30. Schwartz, P.M.: Property, Privacy, and Personal Data. Harvard Law Review **117**(7) (2003) 2055–2128
31. Samuelson, P.: Privacy As Intellectual Property? Stanford Law Review **52**(5) (2000) 1125. https://doi.org/10.2307/1229511
32. Litman, J.: Information privacy/information property. Stanford Law Review (2000) 1283–1313
33. Purtova, N.: Property in personal data: Second life of an old idea in the age of cloud computing, chain informatisation, and ambient intelligence. In: Computers, Privacy and Data Protection: an Element of Choice. Springer (2011) 39–64. https://doi.org/10.1007/978-94-007-0641-5_3
34. Marmor, A.: What Is the Right to Privacy? Philosophy & Public Affairs **43**(1) (2015) 3-26. https://doi.org/10.1111/papa.12040
35. Rotenberg, M., Jacobs, D.: Updating the law of information privacy: The new framework of the european union. Harvard Journal of Law and Public Policy **36**(2) (2013) 605–652
36. Veblen, T.: The Beginnings of Ownership. American Journal of Sociology **4**(3) (1898) 352–365. https://doi.org/10.4324/9781351311441-4
37. Janeček, V.: Ownership of personal data in the Internet of Things. Computer Law and Security Review **34**(5) (2018) 1039–1052. https://doi.org/10.1016/j.clsr.2018.04.007
38. Fairfield, J.A.: Virtual property. Boston Law Review **85**(4) (2005) 1048–1102.
39. Massin, O.: The Metaphysics of Ownership: A Reinachian Account. Axiomathes **27**(5) (oct 2017) 577–600
40. Omoronyia, I., Cavallaro, L., Salehie, M., Pasquale, L., Nuseibeh, B.: Engineering adaptive privacy: On the role of privacy awareness requirements. In: Proceedings - International Conference on Software Engineering. (2013) 632–641
41. Trepte, S., Teutsch, D., Masur, P.K., Eicher, C., Fischer, M., Hennhöfer, A., Lind, F.: Do People Know About Privacy and Data Protection Strategies? Towards the "Online Privacy Literacy Scale" (OPLIS). In: Reforming European data protection law. (2015) 333–365
42. Parliament, E.: Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Official Journal of the European Communities **59** (2016) 1–88