2010

Privacy: An Ontological Problem

Shan Chen
University of Technology, shanc@it.uts.edu.au

Mary-Anne Williams
University of Technology, mary-anne@it.uts.edu.au

PRIVACY: AN ONTOLOGICAL PROBLEM

Shan Chen, Innovation and Enterprise Research Laboratory, Centre for Quantum Computation and Intelligent Systems, University of Technology, Sydney, NSW Australia, shanc@it.uts.edu.au

Mary-Anne Williams, Innovation and Enterprise Research Laboratory, Centre for Quantum Computation and Intelligent Systems, University of Technology, Sydney, NSW Australia, mary-anne@it.uts.edu.au

Abstract

Approaches to addressing privacy issues tend to assume privacy is well understood and typically approach the problem from a security perspective. However, security is more concerned with safety than with privacy. Given the lack of satisfaction with advanced privacy-enhancing-technologies, we argue that an ontological framework is fundamental to advancing the capabilities of technology-enabled solutions. In recognition that privacy is a right to control information about oneself, this paper develops a new ontological foundation for privacy - an initial and important step to modeling privacy as a means to improving the privacy protection effectiveness of information systems.

Keywords: Privacy, Information Privacy, Right to Information Privacy, Ontological Status.

1 INTRODUCTION

Privacy is an important characteristic of information sharing in human societies. Inevitably we give information away about ourselves, knowingly and willingly, because we want and/or need to communicate, share and exchange information with others; unknowingly or unwillingly, because of obligations, regulations enforcement, survival (such as buying goods and employment) or social needs. When information is processed in digital form by information systems - maintaining data privacy becomes a major concern. In particular, in the case of online information, technology-based approaches dominate the privacy literature in the area of information technology that tend to focus on information access control aspects like security. Recent emerging online social networking services typically emphasize the importance of technological issues due to the complexity of the networks' Internet infrastructure. However, the increasing number of privacy breaches reported in the media reveals that the fundamental problem of data privacy protection still remains unsolved despite the plethora of privacy-enhancing-technologies (PETs) available for implementation.

Approaches to addressing privacy issues tend to assume privacy is well understood and attack the problem from a security perspective rather than addressing the underlying ontological problem associated with privacy. There have been many definitions and analyses of "privacy" as a concept; however, clarity and consensus are still lacking. A widely cited definition of privacy is "*the right to be left alone*" (Warren and Brandeis 1890) – privacy in some societies and cultures can be understood as a human right. It is "*the state or condition of being free from being observed or disturbed by other people*" (OAD 2005). In the contemporary digital information era, privacy is naturally reduced to information privacy – "you are your information" – the "states" and the "conditions" of your "rights" are understood and disseminated in the form of information. Accordingly, privacy issues concern the justifications of "states" and "conditions" with respect to individuals' "rights". Such justifications have foundations in Information Ethics (IE) and Philosophy of Information (PI) – both address fundamental ontological problems. The lack of understanding the concept "privacy" and the state-of-the-art of technological solutions suggest that, a deeper appreciation of privacy's ontological status will help to develop a clear and robust set of requirements upon which advanced privacy-friendly information systems can be designed, developed and deployed.

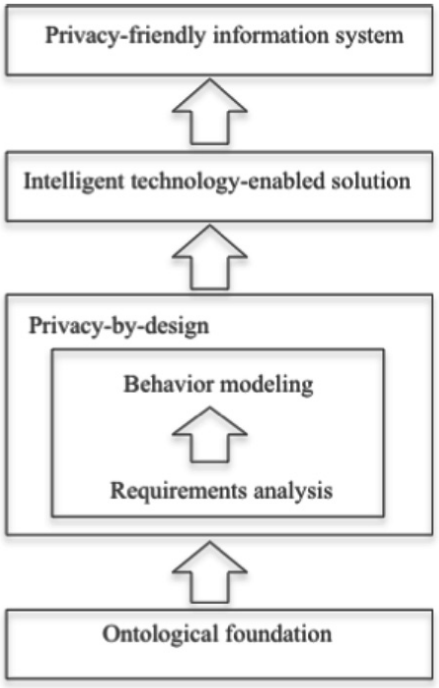

Figure 1. A Methodological Framework for Privacy Protection

Figure 1 illustrates the importance of a firm ontological foundation of privacy is for the development of privacy-friendly information systems. The purpose of this paper is to develop a new ontological grounding of privacy that will lead to a major improvement in information systems' performance and have positive impacts on the quality of service that information systems can achieve in the contemporary era of social computing.

The rest of this paper is organized as follows: Section 2 highlights the pervasiveness and public nature of privacy using example scenarios; Section 3 studies some legal and social dimensions of privacy; Section 4 analyses fundamental ontological privacy problems based on the set of ontological dimensions identified; and Section 5 concludes the study with an outlook.

2 UBIQUITOUSNESS

It is impossible to live in today's society without giving away information about ourselves. We buy food from a supermarket. The storeowner or cashier knows what we are buying. We register relevant information with agencies for purchasing basic infrastructure like power and water, buying goods, searching for jobs, planning/arranging travel, etc. The agencies know our contact details, habits, preferences, plans or intentions. We consult with doctors for healthcare. The doctor knows our health conditions. To illustrate some of privacy issues that arise in everyday life, consider the following examples where we describe two typical scenarios with one related to everyday life in the off-line world, and the other demonstrating how the online world is connected with the off-line world.

[Example 1: Eating habit] I always buy the same type of fish from the same fish market. On New Year's eve I visited the market again but I planned to buy a different type of fish for my family. When I entered the market the owner told me that all the fish I would normally buy sold out but she kept one for me because she knew I liked that kind of fish. It was the first time I felt uncomfortable about her knowing my eating habits because I did not want to take the fish that my mum did not like; however, I felt impolite by not accepting the owner's kindness. At that time I preferred she did not know about my eating habits.

[Example 2: Online vs. Off-line] I have several email accounts to keep personal emails and work-related emails separately, because I wanted to keep my personal life and professional life strictly disjoint for privacy concerns. But I failed to do so after my housemate Katy moved overseas because she likes to send messages to a group of people in one email with email addresses explicitly listed in the CC line. One day I received an email from Tom replying to Katy's travel message. I did not know that the sender, Katy's friend Tom, is my colleague Tom and I hit return to send my opinions regarding Katy's discussion topic. Next an email from Tom reached me asking how I see the new changes to the holiday policies in my company.

3 GROUNDING PRIVACY

A crucial and thus far unanswered question is how privacy should be understood such that clear and detailed guidelines for guarding privacy or developing a privacy-friendly information system can be established. The importance and the role of privacy must first be understood: what is privacy and to what extent is it of value to us? Philosophers justify an object's value as a compound property of intrinsic value and extrinsic value. *Intrinsic value* concerns the value an object has in itself or for its own sake, whereas *extrinsic value* concerns the value that can be generated from intrinsic values. Intrinsic value is absolute but can be contextual, while extrinsic value can be subjective and contextual.

The philosophical value of an object provides a philosophical foundation upon which the importance of privacy can be justified by its value. By its connotation of "rights", privacy has intrinsic value because of its associated "rights" which are fundamental to human dignity (e.g., life, happiness, freedom, knowledge, ability, resource, security, respect, etc.) In human society, individuals develop relationships with dignity and mutual respect. Consequently, privacy has extrinsic value, i.e., the power of rights, which protects us from losing dignity. Without privacy we will not have the

necessary dignity that enables us to build relationships with others in society - as Rachels (1985) states, privacy enables us to form relationships with other people.

3.1 The Nature of Privacy

The intrinsic value of privacy suggests a way to understand the nature of privacy and its scope by using *the situations in which dignity is required* as criteria:

- Natural dignity in a naturally private situation. For example, nobody knows what I look like when I am sleeping.
- Normative dignity in a normatively private situation protected by ethical, legal or conventional norms. For example, nobody knows my consultation (the content and the activity) with my doctor.

Accordingly, privacy with natural dignity and normative dignity are referred to as *natural privacy* (Moor 1997) and *normative privacy* (Moor 1997), respectively. In the natural dignity example, natural privacy concerns the right not to be disturbed and the right not to be observed (if one does not want to be), e.g., when "I" am sleeping; whereas in the case of normative dignity, normative privacy concerns the right to keep the consultation content and information about the consultation activity private.

However, these two categories provide insufficient support in understanding the nature of privacy because they do not detail *situations* in which dignity is determined and obtained. Moor (1997) gave a better interpretation by emphasizing situations as follows:

> "*An individual or group has normative privacy in a situation with regard to others if and only if in that situation the individual or group is normatively protected from intrusion, interference, and information access by others.*"

It can be seen that the key to determining privacy status is the *situation*, which essentially involves *others* (in relation to the privacy protection subject) and further requires justification of *intrusion*, *interference* and *the nature and kind of information access*. This justification is necessary to understand "what is *not* a private situation", which is a mechanism to reach an understanding of "what is a private situation where privacy can be protected".

From a normative perspective, the perception of intrusion, interference and relevance of information access can significantly vary, culturally and spatiotemporally; hence, the difficulty to specify privacy ontologically. Moor (1997) proposed a Core Value Framework (CVF) to uncover common existences in all human cultures as a means to justify the importance of privacy. Values of these existences must be fundamental to human evaluation such that they can be shared by all humans regardless of their cultural contexts. Such values represent human needs, and are thus core to dignity. In the CVF privacy is seen as an extrinsic value to support all the core values for human society. By this interpretation, privacy intrinsically supports human society because it is an expression of a core value namely *security*. In this light, Moor (1997) views all the core values are mutually supporting. We agree with this philosophical stance and furthermore we argue that privacy is not only an expression of security, but also it intrinsically supports all other core values with its own intrinsic value via rights. Subsequently privacy is a core value of humans in society. It follows, to a certain extent, that a personal privacy claim is a publicity claim, which necessarily reveals identification of who is making the claim because such a claim requires recognition from others. In other words, one's perception about one's relationship to others involved in a given situation in which the claim is valid needs to be presented.

A successful identification performed in one context might not be successfully performed in another context. This is because identities are valid only in certain contexts. A situation claimed for occurrences such as intrusion, interference and information access that related to one's privacy status is valid only when one can be identified in the context where the situation occurs. This follows a situation to be claimed for relevant occurrences essentially a claim of *identity* in context and associated *accessibility* (and inaccessibility), which involves a view of one's relationships to others.

Following this line of reasoning, privacy is a form of claim to rights, self-situations and self-identity (typically via relationships), in one's desired status.

With this interpretation, our aim for privacy protection does not align with the common understanding that information privacy is the minimum amount of personal data to be shared – i.e., "data minimisation" as requirements (Leenes et al. 2008). Our approach demands that privacy protection protects one's rights in claiming the *desired status* of information about oneself, while not violating others' rights.

3.2 Dimensions of Privacy Claim

To develop a justification of one's privacy status, this sub-section explores dimensions of concepts relevant to privacy claims, namely, rights, relationships, identities, situations and goals.

3.2.1 Rights

The right to information privacy is the right to control "*who* can **do** *what* to me".

- The *who* concerns one's relationship to others. This concern requires a consideration of situations in which the relationship is valid/recognized. Since relationships evolve over time, a situation is determined spatiotemporally – i.e., when and where, if applicable. Thus, the right to information privacy has a situation dimension – i.e., in what situation can the right be claimed.
- The *what* concerns information content and details its information about "me". The right in this dimension is to determine size, volume and granularity of the "what".
- The *do* concerns actions on the "what" (i.e., the selected information). Do-actions can be observation, presentation, access, manipulation or distribution. *Observation* means watching and remarking on the information, *presentation* refers to the freedom of one in presenting the information (i.e., when, where and how to present the information), *access* means ways of viewing and retrieving the information, *manipulation* refers to modification of the information, and *distribution* means sharing the information out with one or among a number of recipients.

The following three *rights* are required for information privacy (Williams 2009; Chen and Williams 2010a):

- choice – the right to decide if the information is private or public, what information to control, and what action(s) can be performed on the selected information.
- consent – the right to declare (self-)choice to others (what and how to control).
- control – the right to enact the consent.

In summary, the right to information privacy is the right to choose who has permission to do what to enable control of one's information on one's desired status. All rights can be claimed in any of the three dimensions: who, what and do-action.

3.2.2 Relationships

A relationship indicates a connection between at least two entities, directly or indirectly. Such a connection can be symmetric or asymmetric. A relationship is symmetric if entities involved in the relationship share the same attitude of the relationship, i.e., recognize the relationship under the same conditions; otherwise, the relationship is asymmetric. For example, the relationship between *A* and *B* is symmetric if both set the relationship to the same type under the same conditions. The relationship is asymmetric if *A* sees *B* as a friend but *B* sees *A* as a colleague. The asymmetric property implies the existence of *direction* in a relationship. The condition that holds in a relationship is referred to as the *type* of the relationship.

The same social entities can hold more than one type of relationship. For example, *A* and *B* are

siblings, classmates and both are members of The A&B Club. The connection between *A* and *B* is therefore described as "sibling, classmate and The A&B Club member". As a result a direct connection between two entities is *multiplex* if more than one relationship exists between them.

A connection can directly or indirectly connect entities. When two entities are connected indirectly, the connection can be described by the distance between them, and the relationship between all the entities connecting them (i.e., the two entities under consideration). The concept of *connection degree* (Chen and Williams 2009) can be used to indicate the distance. For example, if *A* connects to *B*, and *B* connects to *C*, then *A* is said to be 2 degrees away from *C*, i.e., the connection degree between *A* and *C* is 2. If there are multiple paths connecting *A* to *B*, technically the degree of *A* and *B* is the length of the shortest path between *A* and *B*, because it reflects one's ability to connect to another economically. However, when considering privacy, the length of a connection path is not a dominating factor in assessing a relatioinship; rather, the types of relationships involved in the path have more impact on one's privacy status. The concept of *relationship by connectivity* (RBC) (Chen and Williams 2010b) can be used to describe this complexity of relationships. It describes a set of relationship types between two entities under consideration and the related connection degree from one of the two entities as a reference. In the above example, if *A* and *B* are colleagues, *B* and *C* are friends, and *A* and *C* do not know each other, then the RBC from *A* to *C* is described as a path: {("work",1),("friend",2)}.

Social entities involved in a relationship can be at different levels of abstraction. For example, a relationship can be individual to individual, individual to group where the individual can belong to the group, group to group where one group can belong to another group or they can overlap or be completely disjoint. Thus, a relationship has an *abstraction level*, explicitly or implicitly.

In summary, a claim of relationship needs to include status of direction, type, multiplex, connection degree and connectivity (i.e., RBC).

3.2.3 Identities

According to the Oxford dictionary (OAD 2005), identity is "*the fact of being who or what a person or thing is*", or "*a close similarity or affinity*". Commonly it is understood as something a person or thing has that distinguishes themself from others.

Physical properties form natural identities for all beings. Humans are beings that have social requirements - in fact, social ability and physical needs. In human society, identities are often seen as social identities. In Appiah's (in Taylor 1994) view, a social identity has *collective* and *personal* dimensions. In a society, an individual often belongs to various social categories (e.g., categories of qualification, profession, leisure, race, gender, religion, etc.) where the individual is judged by others to fit in. This judgement reflects others' view in recognizing the individual's collective position; therefore, it can be seen as an identity of the individual in the collective context under consideration, i.e., collective identity. The *collective dimension* of one's social identity holds the intersection of one's collective identities. Analogically, the *personal dimension* holds the intersection of all social properties that do not comprise a social category (e.g., intelligence, attractiveness, objection, etc.) Both dimensions intersect a complete social identity. By emphasizing the "social importance" of properties as a criterion for social identities, Appiah sees a property as part of one's identity essentially relies on others' response to the property. This view largely reflects the fact that identities are generally valid only in certain contexts – i.e., an identity valid in one context might not be valid in another context. This fact is evidenced in many everyday's scenarios. For example, a student ID of University of Technology, Sydney (UTS) is valid at UTS but not valid at other universities, a driver license is valid in the state of NSW but not in the state of VIC, an UTS fitness membership is valid at the UTS Fitness Center but not at the Broadway Fitness Center, just to name a few.

Another relevant view is the concept of *partial identity* (Pfitzmann and Hensen 2007), which is a subset of a complete identity. In a certain context, a partial identity can serve as a full-fledged identity of an entity, and can be a collective identity if it is valid in a collective context. In reality, this is not necessary always the case because a partial identity can contain more or less information than a collective identity requires. Thus, partial identities can be recognized in wider or narrower contexts than a collective context of a complete category. On the other hand, unlike collective identities that

are recognized collectively, partial identities mainly rely on the entity whose identity is under consideration about how he/she wants to be identified by others in order to connect to them on a desired relationship. In other words, partial identities reflect how the data subject intends or is allowed to interact with others within the context in which the partial identity is valid – as studied by Goffman (1959), partial identities are revealed by the individual with concerns of what part of self-identity is prepared to show to the world (i.e., an intended context) and therefore it is essential to keep contexts separated for partial identities. Rachels (1985) states such separation of contexts allows different types of relationships.

On the other hand, because partial identity is subdivided from a complete identity with intended purpose (i.e., to be used in an intended context for maintaining certain types of social relationships for social interactions), they can blur the boundary between social dimension and personal dimension. The concept of situation described in the next sub-section can be used to reclaim the boundary for privacy justification.

3.2.4 Situations

Situations show how relationships and relevant privacy occurrences are situated in context, and thus determine their status. We define the term "situation" as an instance of a sub-context. In other words, multiple situations can co-exist in a context. In an intended context where one's identity is created, occurrences are relevant to privacy when any of the identity information is used unexpectedly. Such occurrences include positive do-actions like welcome services and negative do-actions like intrusion, interference or invasion. What conditions can trigger these events? When an event is triggered, what is the subsequence of actions that will follow? A situation is determined by the status of all properties that can answer these questions. Thus, a situation has an occurrence dimension.

An occurrence affects the environment only when an *actor* activates it under certain *conditions*. It remains active in those circumstances. An occurrence may or may not have co-occurrence that may or may not affect the environment. A *privacy occurrence* is an occurrence that affects one's privacy status. The actor of such an occurrence can be the person whose privacy is under consideration, or not. The impact of an occurrence can be positive or negative. For the purpose of privacy's ontological status, we only consider occurrences that will generate negative impacts on one's privacy. Since privacy is a claim of one's desired status about one's information, a privacy occurrence is a claim of one's believes of its impact on one's privacy status. Thus, a claim of a privacy occurrence claims the type of the occurrence that distinguishes from other occurrences, actors who triggered the occurrence, conditions under which the occurrence is active, reasons about the claim, co-occurrences as subsequence of the occurrence (if any), and implications that one believes that will occur. Since the claim of actors is a claim of one's relationship with them, i.e., actors are claimed via the span of relationships, a situation has a relationship dimension.

3.2.5 Goals

Goals indicate desired results. Goals of privacy reflect one's desired privacy status. While privacy is subjective and highly person-dependent, there are common goals for human beings' privacy as a value to support core values intrinsically and extrinsically. In other words, there are common desired results for privacy for all human beings. Consider core values namely dignity, security, ability and resource, common goals expected to support these core values typically include:

- Awareness – one is aware of one's rights and situations.
- Anonymity – one's ability to undertake an activity without being identified.
- Pseudonym – one's ability to undertake an activity without being "physically" identified by one's actual identity.
- Self-Partition – one's ability to partition one's identity for different contexts.
- Integrity – one's ability to prevent information from being misused without one's permission.

- Unobservability - one's ability to be free from being observed.
- Unpresentability – one's ability to prevent one's information from undesired presentation.
- Inaccessibility – one's ability to prevent one's information from unwelcome access.
- Inmanipulatability – one's ability to prevent one's information from unwelcome modification.
- Indistributability – one's ability to prevent one's information from those who has access privilege distributing the information to third parties.
- Unreachability – one's ability to prevent one's information from being reachable upon an absence of one's consent or biased preferences.
- Unlinkability – one's ability to prevent one's information in different context from being linked together.
- Confidentiality – one's information is kept confidential during transfer from one location/party to another.
- Liability – one's obligation as a fundamental requirement to realise all the goals above.
- Accountability – one's ability to justify all the goals above on one's core values.

These goals support all the core values from different aspects. Goals can be claimed separately, jointly, or a combination of both. A claim of one goal might lead to a claim of other goals, implicitly or explicitly. Detailed analysis of the interplays between goals will be presented in the next section.

4 ONTOLOGICAL STATUS

Figure 2, below, shows the relationships between dimensions that ontologically describe the intrinsic and extrinsic properties of privacy. In the following we describe these dimensions and their interaction in detail.

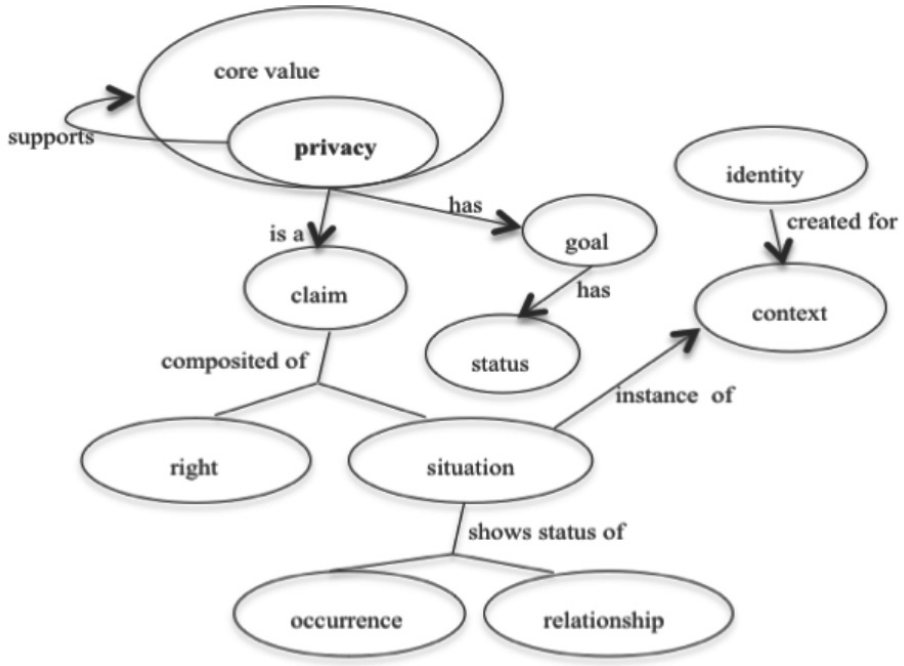

Figure 2. Ontological Grounding of Privacy

Rights

One's right to information privacy is the right to control what others can do with information about oneself. The *do* actions are common actions that can be performed on information where privacy might be infringed, i.e., actions can impact information's known and used status. One's ability to

control one's information is to determine who can perform what action. Allowing *distribution* automatically grants permissions for *access*, *presentation* and *observation*, and can also lead to a permission for *manipulation*. A permission to *access* grants permissions for *presentation* and *observation*.

Permissions not only can be transferred between actions, but also actors – i.e., the *who* object. Since this object reflects the one's relationship to others, the transferability of permission is determined by the relationship.

Identities and Relationships

An identity is valid when the information it carries is sufficient to identify an entity in the intended context. The validity of a collective identity relies on the validity of the social category where the identity exists. If a collective identity is made available outside the social category, a claim of the identity will reveal the individual's relationship to the social category, and therefore relationships to those in the same social category. A partial identity may or may not be valid in the context where it is intended because partial identities may be made available by the individual whose identity is under consideration. They may be subjective due to the unawareness of the intended context. For example, intended relationship types, networks, situations and their implications, etc.

With the purpose that relationships between the individual (whose partial identities are under consideration) and others' can be established and maintained, partial identities are created by making a subset of an identity available in a context where some others have access. Such a purpose provides a way to discover identity via relationship (either existing ones or potential relationships). A claim of identity implicitly makes a claim of relationship.

Relationships can be infinite like kinship. Most relationships have a lifetime with start date and end date, and other conditions bound to it. Conditions can include *obligations* that entities of the relationship must carry on in order to be tied to the relation. Obligations on an asymmetric relationship can be different for the entities on the relationship. In other words, obligations can be asymmetric for an asymmetric relationship. When entities are involved in other relationships, the obligation may be inherited by other entities that connect to them. Asymmetric obligations can lead to permissions transferred to those connecting to them. Situations that involve such occurrences can easily lead to situations where information flow along unexpected or unintended pathways and resulting in an increase in uncertainties of obligations and permissions.

Social referrals are common activities in human society. They naturally introduce indirect social connections. When one entity connects to another via a referral, a new connection is established indirectly. Such a connection can be implicit if the entity being referred was not aware of the referral. Such implicitness creates an accountability privacy problem (i.e., the goal of accountability). When the indirect connection is developed to a direct connection and the referred entity remains unaware of the previous situation (i.e., one is not aware of one's information being made known to the other party), negative privacy occurrences or unexpected do-actions may occur.

Situations

A situation describes a state of affairs. It has a time and a location attribute. Thus, a situation shows static relationships. Each relationship is identified by a type, a direction and a connection degree. A relationship situation reflects the connected entities' *views* on the relationship. For example, *A* and *B* are "friends" and both agree to keep each other's personal information confidential. They both work for the same company where *A* is in the marketing department led by *B*. One day client *C* called *A* on her mobile for a potential contract. *A* was surprised that *C* knew her personal mobile number. *A* then received a call from *B* who said that he gave *C* her number because that would be a potential big contract for the company. *A* was upset that *B* saw her as a colleague more than a friend. At the time *A* received the calls from both *B* and *C*, *B* exposed his attitude towards his relationship with *A* as "colleague" not "friend". From this example we can see that a claim on actors via relationship is a claim of the actor's view.

From a static perspective, an occurrence situation shows the pre-condition or the post-condition of an event or action at a particular time. For example, a *lost* occurrence indicates one lost some privacy as a result of some information being made known to unintended parties or given to wrong hands. It is a result of "make known" or "use" actions. Although, it can also be a pre-condition for subsequent events or actions. For example, loss of privacy can lead to privacy-invading actions.

Most occurrences related to one's privacy have actors other than oneself. Such actors are typically explicitly or implicitly, connected to the individual whose privacy is under consideration. When there is more than one actor of a negative occurrence, the occurrence situation can explain a potential *privacy-invading network*.

Situations can be isolated or overlapping. A situation is isolated by unique status uniquely described by all its properties, i.e. an isolated situation is disjoint from any other situations. Situations overlap when they are not disjoint. The interplay between situations complicates the justification of one's privacy status and can result in failures of claiming privacy rights. The complexity of situations lies in:

- A situation instantiated by a partial context of a complete intended context may not recognize one's identity. Claiming occurrences in such a situation is difficult to justify.
- A claim can across multiple situations with current or past time-stamps. A situation can be an abstraction of other situations. If a claim is associated with an abstract situation, justification must be based on all situations (and related) that support the abstract aspect of the situation being claimed.
- Situations can be used to infer other (possible) situations. For example, in a situation where information is lost, intrusion, interference or disturbance occurrence(s) can result in an invading situation. A claim for maximum rights (privacy) needs be intelligible to include "future situations" in accordance with potential inferences.

Situations related to oneself include not only the above complex scenarios, but also necessary situations for those who are in one's potential privacy-invading networks. A successful claim of one's privacy right needs to be made on all possible situations. However, in a complex social environment – i.e., large, open, dynamic and complex social networks, it is impossible to learn all the possible situations. One needs to justify one's position in the network based on some criteria. Thus, a theory is required.

Goals

One's awareness of one's privacy status is a fundamental goal, without which one will not be able to adapt other goals in a dynamic environment. Anonymity, pseudonym and self-partition ensure integrity of identities: i) both anonymity and pseudonymity achieve confidentiality of an identity and reserve completeness of the identity, and ii) self-partition reduces the chances of misusing one's identity by subdividing it based on context.

A pseudonym creates an anonymity version of collective identity. Self-partition generates partial identities by contexts. Such a partial identity may or may not be a collective identity – detailed discussion of these two types of identities was presented in the previous sub-section.

Pseudonyms can introduce overheads if one creates different types of pseudonyms for different contexts, where there are overlaps; particularly, when accessibility or distributability is granted for those who can reach, observe or access other contexts that are disjoint with the pseudonyms' contexts. The same is true in partial identity overlaps. In these cases, pseudonym/self-partition affects achievability of other goals, and in turn rights of the individual whose identity is under consideration may not be successfully claimed.

Reachability does not guarantee accessibility. It reflects only probabilities of being reached from where and/or by whom. Therefore inaccessibility does not imply unreachability. One must be able to reach another in order to observe him/her. Thus, observability requires reachability; and unreachability warrants unobservability where unreachbility includes unlinkability. For example, *A* talked to *B* about *C* when *A* did not know *C* personally (i.e., *A* does not have *accessibility* to *C*).

However, *A* was able to observe *C*. Through the communication with *B*, *A* enabled *B*'s *observability* on *C*. If later on *C* granted *A* accessibility to his information and *A* talked to *B* again about *C*, *B* was not able to grant accessibility on *C* from the second communication between herself and *A*. In other words, observability can be transferred but accessibility cannot be transferred without permission because accessibility includes observability; a transfer of accessibility permits transfer of observability. Moreover, observability comes with reachability; a transfer of observability includes a transfer of reachability. Thus, unreachability includes unobservability, which implies inaccessibility.

Distributability enables accessibility, and follows observability and reachability. One's goal to prevent others from distributing one's information must include not granting accessibility to those under one's consideration. Distributability can also come from observability because one can distribute what one observes even though one has no access to the information. In the above example, *B* does not have accessibility to *C*, however, she can distribute what she has observed about *C* to others. Thus, one needs to assure inaccessibility and unobservability to realise indistributability.

Without achieving confidentiality one will not be able to obtain desired status of one's information. One may be able to achieve unreachability, unobservability, inaccessibility and/or indistributability; however, if one fails to keep the information desirable attributes that where reachability, observability, accessibility and/or distributability are enabled, information leaks will be possible. For example, if *C* granted *A* a distribution permission to distribute his information to *B* and *A* passed the information to *B* without noting *D* was within the distance of hearing, then *D* would receive the information about *C* – i.e., *C*'s information was leaking – an undesired result that against *C*'s goals of achieving unobservability on *D*.

Many types of information can be partitioned into parts. Some parts may have the same impact on one's information privacy status whereas some may not affect the status or have different types and/or degrees of impacts. Use of the complete information and use of portions of the information can result in different privacy statuses of one's information. On the other hand, from a contextual perspective, integrity ensures information is used in the permitted context(s). Information permitted to be used in a sub-context of an intended context, or in an unintended context, can result in undesired status of the information. Thus, the integrity of information is essential to achieve one's privacy goals completely.

5 CONCLUSION AND OUTLOOK

Privacy concerns focus on "who can do what to me". In human society, privacy is ubiquitous. Its pervasiveness and public nature highlight its legal and social foundation which has a philosophical root. Without developing an ontological foundation for privacy it will continue to be difficult to achieve practical advances in effective privacy protection technologies. Current privacy-enhancing-technologies (PETs) lack support for modeling the necessary rich legal and social expectations. In fact they put a major emphasis on *security* rather than *privacy*. Security is more concerned with safety than with privacy. To bridge this research gap, we propose a methodological framework (Figure 1). This framework takes an conceptual approach to advancing the ontological foundations of privacy as a basis to support effective privacy requirements analysis, which in turn supports the development of innovative privacy-by-design (Cavoukian 2010) models. Privacy-by-design has been identified as an open issue in privacy-friendly information systems (Williams 2009; Chen and Williams 2010a; Cavoukian 2010). Privacy-by-design models can be used to develop technologies that can support user behaviours and assist users to learn and manage their privacy more effectively.

As an initial step to implement this framework, we analysed fundamental ontological characteristics of privacy. We provided a new ontological understanding of privacy from its legal and social foundations namely *rights* and *relationships*. We then identified relevant concepts that are related to these two core concepts, namely, identity, situation and privacy goals. Future work will build on the new ontological foundation and focus on privacy-by-design models with intelligent capabilities to address the problem of developing robust privacy-friendly information systems and to provide the necessary support to users which will allow them to give informed consent, to control and manage the privacy of information content.

References

Cavoukian, A. (2010). www.privacybydesign.ca/publications.htm. (Accessed on 19 March 2010).

Chen, S. and Williams, M.-A. (2009). Privacy in social networks: A comparative study. In *PACIS 2009 Proceedings.* Paper 81.

Chen, S., and Williams, M.-A. (2010a). Towards a comprehensive requirements architecture for privacy-aware social recommender systems. In Link, S., and Ghose, A., eds., Proceedings of the Seventh Asia-Pacific Conference on Conceptual Modelling (APCCM 2010), 33–41. Australian Computer Society Inc.

Chen, S., and Williams, M.-A. (2010b). Modeling privacy requirements for quality manipulation of information on social networking sites. In Proceedings of the AAAI-SSS10. Intelligent Information Privacy Management.

Goffman,E. (1959) The Presentation of Self in Everyday Life. Anchor Books, June 1959.

Moor, J. H. (1997). Towards a theory of privacy in the information age. *SIGCAS Comput. Soc.* 27, 3 (Sep. 1997), 27-32.

Leenes, R. , Schallaböck, J. and Hansen, M. (2008). Prime white paper v3. *Technical Report, PRIME Project*, May 15, 2008.

OAD (2005). Oxford American Dictionary, 2005-2007, Version 2.0.2(51.4) Apple Inc.

Pfitzmann, A. and Hansen, M. (2008) Anonymity, unlinkability, undetectability, unobservability, pseudonymity, and identity management – a consolidated proposal for terminology, February 2008.

Rachels, J. (1985). Why privacy is important. In *Ethical Issues in the Use of Computers* Wadsworth Publ. Co., Belmont, CA, 194-201.

Taylor, C. (1994). The politics of recognition. In A. Gutmann (Ed.), Multiculturalism: Examining the politics of recognition (pp. 25–73). Princeton, NY: Princeton University Press.

Warren, S., and Brandeis, L. (1890). The right to privacy. In F. D. Schoeman (Ed.), Philosophical dimensions of privacy: An anthology (pp. 75-103). Cambridge, UK: Cambridge University Press.

Williams, M.-A. (2009). Privacy, the law and global business strategies: A case for privacy driven design. In Proceedings of the AAAI-SSS09, Social Semantic Web: Where Web 2.0 meets Web 3.0.