7-15-2012

Information Makes A Difference For Privacy Design

Shan Chen
Innovation and Enterprise Research Laboratory, Centre for Quantum Computation and Intelligent Systems, University of Technology, Sydney, NSW Australia, shan.chen@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-anmary-anne.williams@uts.edu.au

INFORMATION MAKES A DIFFERENCE FOR PRIVACY DESIGN

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

Abstract

In the current information age, information can make a difference to all aspects of one's life, emotionally, ethically, financially or societally. Information privacy plays a key role in enabling a difference in many dimensions such as trust, respect, reputation, security, resource, ability, employment, etc. The capability of information to make a difference to one's life is a fundamental factor; and privacy status of information is a key factor driving this difference. Understanding the impact of these two factors to one's life within an IS context is an important research gap in the discipline. This paper studies "information + privacy", ontologically and integrally, in making a difference to one's life, within the IS context. In recognition of the importance of the Privacy-by-Design approach to IS development, a methodology is proposed to understand the grounds of information and model fundamental constructs for using Privacy-by-Design approach to develop robust privacy-friendly information systems.

Keywords: Information, Information Privacy, Information Paradox, Core Value, Privacy-by-Design.

1 INTRODUCTION

In information systems (IS), information is the primary resource and motivation for systems and their users. The types of information the system is able to or intends to collect, store and process motivate the system's design, development, deployment and maintenance. The types of information the user can access and manage, and the way to do so, motivate users to interact and the way to interact with the system. These motivations show initial differences information *can* make when it enters the practice of IS domain. Given the existing wide range and diverse of IS application systems, further differences can follow, diversely, in specific application domains. Consider two social networking systems that collect users' contact details, one with default opt-in and the other with default opt-out options. A difference to the user's privacy of their contact information can be made in-between the default opt-in and the default opt-out; in particularly, for those *unconditionally* accept system defaults. Such a difference to privacy can lead to a difference to security in protecting users from being reached by unwelcomed parties (via access to their contact information); and consequent differences to the user's other social values/positions like trust, respect, resource, ability, opportunity, etc. When information makes a difference to one's privacy, it makes subsequent differences to one's other relevant social values/positions; and vice versa. These values are fundamental to human users, meaning that ontologically they are common core values to all users regardless application domains.

The capability of core values (CVs) to address privacy issues has been demonstrated by a number of researchers (Moor 1997; Chen and Williams 2010b). In the attempts to uncover common existences in all human cultures as a means to justify the importance of privacy (Moor 1997) and ontological grounds of privacy as a means to derive privacy requirements (Chen and Williams 2010b), these works have built an ontological argument for developing CV-based methodologies to manage information privacy and to develop privacy robust information systems.

In today's Web 2.0 enabled information age, user self-created information can make a difference to their personal privacy has been evidenced by many privacy-invaded cases reported in the mainstream media (e.g., France-Presse 2007; Moses 2009). This phenomenon has stimulated the need to manage information on its capability of making a difference to its stakeholder's privacy. This paper seeks to advance understanding of information from the stance of making-a-difference within the scope of the Core Value Framework (CVF) proposed by Moor (1997) and its extension developed by Chen and Williams (2010b), aiming for a methodological framework for implementing privacy-by-design (Cavoukian 2010) requirements upon which advanced privacy-friendly information systems can be designed, developed and deployed.

The rest of the paper is organized as follows. Section 2 scopes the problem domain; Section 3 presents a methodological framework; Section 4 presents forms of information's existence and social channels of information within the scope identified; Section 5 remarks differences from three clusters of information; Section 6 proposes a model of privacy construct for IS development based on the findings. Finally, Section 7 presents concluding remarks and identifies future work.

2 PROBLEM DOMAIN

The problem domain of this paper is "information" and "privacy". This section identifies the scope in these two dimensions.

2.1 The Notion of Privacy

The concept of privacy has many underpinning meanings and perspectives. It has been "used denotatively to designate a wide range of wildly disparate interests" (BeVier 1995). Among the many

definitions and notions in the literature, we have argued, within the existing legal and sociological framework, one's privacy is his/her desired status of the information about his/herself (Chen and Williams 2010b). This notion is employed in this paper when privacy is referred to.

2.2 Information

Information plays a dominant role in privacy status. This subsection uses a simple communication example to uncover the capability information has to play a crucial role in its stakeholder's privacy and proposes a path to tackle the challenge.

2.2.1 A Communication Example

Consider a simple communication example:

|| *Tom told Phoebe: "Mary is very sensitive."* ||

Let us learn the communication with a technical mind[1]: the information Tom sent to Phoebe is a simple form that says "A *is* B", which captures one of Mary's characteristics, namely *sensitive* at the degree of *very*. However, if we consider this form with social implications of the information from a communication's perspective, we can see it is unable to deliver the message – e.g., unable to give answers to:

- Mary is sensitive in what sense?
- Sensitivity often has impacts on behaviors. E.g., Mary was sensitive so she was suspicious and difficult to communicate? easy to get hurt? or perceives things with bias? etc. So,
    - What content Tom *wanted* to deliver to Phoebe? Did he *just* transmit what he believed to Phoebe or did he *intend* to influence her impression about Mary - e.g., to stay certain distance from Mary?
    - How would Phoebe *interpret* the message? Without Tom's further explanation how the message was interpreted and used by Phoebe?

Further, regardless what answers will be, Mary's reputation and trust from Phoebe, and her privacy (e.g., as a consequence of reputation and trust) on this personal characteristic, will be adjusted. Such implications will not be captured by the form.

2.2.2 The Paradoxical Problem

The communication, above, demonstrates information's fundamental feature: social influence – i.e., every information has some social purpose. In this example, the information shows Tom's social purpose on Phoebe towards Mary. From a communication's perspective, the social influence is a sender-receiver problem. To the minimum extent, the social feature connects a "sender" and a "receiver". The social influence within the sender-receiver framework is two-fold:

- Social enabling – information can enable the receiver to sharp his/her thoughts, change behavior and/or conduct activities within context.

    E.g., Tom's information enables Phoebe to sharp her thoughts about Mary to some extent in relevant dimensions (e.g., general socialization, collaboration, or business partnership).

- Social constraining – information can constrain the relationship the receiver towards the subject of the information and/or other parties involved in context.

[1] A technical mind considers problems within a large technical extent, e.g., information retrieval, information extraction, clustering, data mining, etc., where the form of information is sufficient for technologies to extract patterns within context.

E.g., regardless what content of the information Tom wanted to transmit, if Phoebe interpreted the information negatively towards Mary and intended to stay distant from her, then, the information is socially constraining towards the relationship between them (in the direction of Phoebe towards Mary) - which in turn socially constrains Mary's access to Phoebe, and consequently resource via or dominated by Phoebe); and vice versa (from Phoebe to Mary).

We refer to the coexistence of social enabling and constraining features of information's as an enablement-constraint paradox[1]. This paradox features information a social paradoxical property[2].

In the cyber world, today, powered by Web 2.0 technologies, information is largely created by cyber users via their cyber activities - directly or indirectly; knowingly or unknowingly. Cyber users are human agents' cyber representatives - i.e., their personae in the cyber world. In other words, human agents are the main drivers and/or causes of cyber activities. This linkage - human agents as cyber actors - indicates a connection between human agents and cyber users; however, blurs the boundary between the cyber world and the physical world for the information stakeholder. This boundary blur adds a boundary issue into social feature of information and its "living environment" follows to evolve, from its original cyber world or physical world to the cyber-physical integrity. This evolution introduces a cyber-physical dimension into information's social influence. As a consequence, the social feature of information extends itself to serve human agents' social activities in the cyber-physical world and functions them as cyber-physical entities. In what follows, social enabling and constraining can take effect across the boundary between the cyber world and the physical world – i.e., information created by cyber users can enable their cyber socialization, ability and opportunities, but can *also* constrain their human agents in the same dimensions; and vice versa. Information from one world can span its social paradoxical effect across two worlds creating a cyber-physical paradox.

2.3 A Path to Privacy Design: On Information Capability

The paradoxical property establishes information a crucial role in major social dimensions (such as trust, respect, reputation, security, etc.) of its stakeholder; and therefore, crucial to the stakeholder's privacy. Given information is the primary resource for information systems, building robust privacy-friendly systems necessary utilizes information's capability into privacy design. In this paper, we propose a path to privacy design for IS on information capability:

Step 1. Identify the scope information can made a difference (Section 3).

Step 2. Identify privacy-relevant social values to which information capable to make a difference (Section 3).

Step 3. Identify the form of existence and the environment the information lives within the scope identified in Step 1 (Section 4).

Step 4. Identify the type of information capable in making a difference, in the context of network-based IS within the scope identified in Step 1 (Section 5).

Step 5. Identify the type of differences can be made to one's privacy-relevant social value (i.e., one's status in his/her social dimensions) (Section 5).

Step 6. Conceptualize and model constructs that are privacy-relevant from the findings above (Section 6).

---

[1] The term "paradox" here is understood in a literal sense, not a logical sense.

[2] This socially paradoxical property of information is acknowledged as an extension to Shannon's (1948) observation that information is constraining and enabling.

3 METHODOLOGY

This section presents a methodology for evaluating privacy using the CVF-Extension (Section 3.1) via the lens of "Information-as-a-Difference" (Section 3.2). Figure 1 shows steps and components of the methodology.

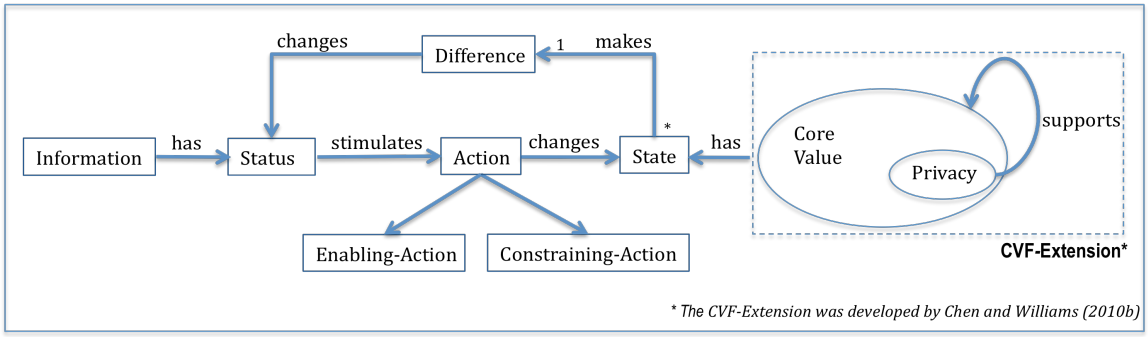

Figure 1. A Methodological Framework for Evaluation of Information-as-a-Difference to Privacy

3.1 Core Value Framework

Privacy is personal-dependent and highly situated, since the perception of intrusion, interference and relevance of information access can significantly vary, culturally and spatiotemporally; hence, the difficulty to specify privacy ontologically. The Core Value Framework (CVF) was proposed by Moor (1997) to uncover common existences in all human cultures as a means to justify the importance of generalized privacy. In this framework, values of these existences are 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 therefore, core to human agents as individuals. Within 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. Chen and Williams (2010b) further develop the framework to 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[1]. Based on this philosophical stance, we scope our privacy problem as the problem of privacy core value in the CVF. We focus on a set of 8 core values, namely, *dignity*, *privacy*, *security*, *trust*, *respect*, *resource*, *ability*, *opportunity*; that are inter-related and coherently an integrity of one's life, and that supports and require supports from privacy - as shown in the CVF-Extension in Figure 1.

3.2 Information-as-a-Difference

The social feature has positioned information a key candidate for fulfilling human agents' CVs. We refer to the state of an individual's CVs as the subject of "difference". Upon this notion, we use the term "information-as-a-difference" to describe information's capability of making a difference[2] to its stakeholder's privacy status via his/her CVs. For example, on receiving Tom's message that Mary was

[1] We refer to the inclusion of this argument as CVF-Extension.
[2] This notion of information-as-a-difference is motivated by Bateson's (1972) postulation in which information is defined as "a difference which makes a difference".

very sensitive, Phoebe's respect towards Mary was decreased. In this case, the information Phoebe received made a difference to Mary's *respect* from Phoebe.

As mentioned in Section 2.2.2, the social feature enables information to generate social influence within a sender-receiver framework. From a sender's stance, information is understood as social signals carrying intended meaning to *re*-present a piece of the world; whereas, the social signals carrying unintended (opted, unintentionally) meaning to interpret the world from a receiver's stance. Understanding information from this sender/receiver-dependency angle information is inward-forming relying on human agents' mental status about the world in which the information takes effect. Such an inward-forming nature places a link between information content and the CVs of human agents involved - as a social signal, information's content depends on the CVs - ability, resource, opportunity, trust, respect, security, privacy, dignity - of the sender for intended meaning or of the receiver for opted meaning. This is an ontological separation between core values attached to or accepted by the human agent to whom the social signal takes effect. The sender constructs the social signal by self's *ability* to use available *resources* to justify self's intension (on *trust*, *respect* and *privacy*[1] - if any - about others) towards the receiver. The receiver, on the other hand, unpacks the social signal by self's *ability* to use available *resources* to adapt self's mental status (on *trust* and *respect* towards the sender, and on *privacy*[2] about self and others - if any) about the world to which the arriving (accepted) social signal interprets. Such social influence between sender and receiver via their CVs implies that, to a large extent, CVs are mainly constituted by the stakeholder's social value in related dimensions. For this reason, we refer to the state of a CV as its stakeholder's social values in the associated dimension. E.g., the state of CV security, is the stakeholder's social value in his/her security dimension.

Unlike quantifiable values, social values cannot be quantified. In addition, social value can significantly vary on context and difficult to qualify. To justify how information can make a difference to its stakeholder's privacy status, we take a CV-based-difference implication approach to identify the most influencing CV by the information under consideration and its impacts on other CVs that can lead to a subsequent difference made to the privacy status. For example, when information is a difference in quantifying one's financial status, it is a difference to qualify one's financial-relevance like purchase or investment *ability*. When information qualifying one's reputation, it makes a difference to others' (awareness of) *respect* towards one - e.g., "She has a high reputation in the community" makes a difference to others, who previously unaware about the information in this regard; and consequently these *others* adjust their trust and respect towards *her*, and might lead to adapt resources made available to her within their availability, creating possibility to further difference made to *her* opportunity, ability, dignity and privacy. When the difference qualifying one's accomplishment, it makes a difference to one's eligibility in context - e.g., "Mary is a lawyer", "Phoebe won the mathFun first prize". When the difference qualifying one's dignity and privacy rights, it makes a difference to one's privacy - e.g., "She is sensitive to her past with that boy"; when the difference qualifying one's privacy status, it makes a difference to one's CVs, and a subsequent difference to one being an individual - e.g., one's mobile number, date of birth, residential address are made accessible to unauthorities - e.g., Vodafone customers' details were made public online (Vodafone 2011), one's privacy on this information, and information that can be accessed by using (any of) these information is updated towards negative consequences - i.e., loss of privacy or privacy can be invaded. This privacy update can make subsequent differences to one's other CVs (compare to the CVs prior to the privacy update) - e.g.,

- security – e.g., financial security (financial-relevant information can be accessed), residential security (residence can be approached without authority).

[1] A privacy stakeholder is whom the subject the information intended.
[2] Privacy here is understood as one's goal for the status of information about oneself (Chen and Williams, 2010).

- ability – e.g., to continue use the mobile number for self-control purpose, to control authority access to residence, to use date of birth to constitute security code.
- resource – e.g., lesser resource available to access leads to lesser ability to control information about the self, which means lesser chances can be obtained to use these information as resource to access service – which, leads to further decrease of available resource.
- trust/respect – e.g., change of security situation, ability and resource can impact trust and respect towards the stakeholder. E.g., unable to stay secure, insufficient ability to keep relevant information secure, or less resource can be obtained can decrease trust towards the self (trust on subjects of interest).
- dignity – e.g., the ability to control abuse of these information.

In line of the ontological argument of Chen and Williams (2010b), these core values *can* stimulate a change of one's privacy core value; thus, a difference made to these core values can stimulate a difference to privacy - i.e., a second update to privacy difference[1].

In what follows, information-as-a-difference to an individual's privacy, via making differences to his/her CVs, which are made within a sender-receiver framework (SRF). In other words, information makes a difference to privacy via CVF and SRF. In what form information exists and via what channel information can flow (i.e., from a sender to a receiver) to generate social influence, within SRF? The next section describes forms of information existence and social channels of information flow.

4 EXISTENCE AND SOCIAL CHANNEL

As humans we are social entities and have social needs (Chen and Willaims 2010b). We develop meanings and signal them - with purposes to influence, and with beliefs to transform, to others. We generate, receive and process information, to make and maintain a difference from others, to live as individuals. Information about ourselves necessary exists during our lifetime; however, information emerged from within our lifetime can continue to exist or be evolved to make new differences. We receive advice from seniors, we learn wisdom from ancestors, we grow and become wise - we become a different person. We develop our own knowledge and share with others, information in our lifetime also exists in others'.

When information exists in the cyber world, digital formats with advanced technologies allow the information to exist infinitely. The vague boundary of the cyber world and the physical world makes physical information cyber-available; and vice versa. E.g., Phoebe's cyber-self's persona for her online travel agent constitutes her flight-booking behavior like her favorite departure time at midnight and arrival time at around noon. This information enables her to receive services tailored to her favors from this agent's website to save time and receive best promotion price. It may also enable her agent's market analysis, customer retention and third-party collaboration. This information contributes to the constitutions of Phoebe's persona. If Phoebe cancels her account with this agent, her persona will expire. However, her information will continue to exist in her agent's database maintained for their former customers, and can continue to be used by her agent market analysis; and third-parties, if any; or, others can describe her persona online elsewhere (regardless if presenting the truth).

It can be seen, from this scenario, that information *can* exist outside of the information creator's lifetime and exists in others'. From one receiver to another, information can be *propagated* and its meanings can *evolve*, from intended to opted; typically, through channels of:

[1] In referencing to the first privacy update in terms of loss of privacy or privacy being invaded.

- communication - information is transferred between the sender and the receiver, directly.

  E.g., information generated by Phoebe is transferred to her agent, a service agent transfers customers' information to a third-party, etc. A shift of information receiver can incur a change of usability – e.g., for Phoebe the information is used to receive better services, for the agent the information is used to better manage business, and for both the agent and third-parties the information is used to gain better profit, etc.

- dissemination - information is transferred through mediators before reaching the intended recipient. Each mediator resets the intended meaning on its opted meaning and re-presents to next receiver. E.g., the agent captures information it values to transfer to third-parties.

The meaning of information is interpreted by the receivers based on their ability, trust and respect towards the sender and the secure level of the arriving channel. Regardless whether the sender's intended meaning can be transferred to the intended recipient end will largely depend on the mediator's core values to re-present the information (the application of the CVs).

When information is transferred to from one end to another, its meaning will evolve to the receiver's interpretations. Such interpretations are formed with influence from the receiver's trust to the sender's reputation to the subject of the information and the arrival channel's security level; and the receiver's ability to understand the information based on available resource - in short, interpretations can turn out variously, on the receiver's core values. In what follows, information *exists-on* meaning and meaning *exists-on* core values and social channels.

5 CYBER-PHYSICAL DIFFERENCE TO CORE VALUES

The type of information and ways of communication or dissemination are key factors for information-as-a-difference to its stakeholder during its existence. This section analyzes three types of cyber-user generated information and the information's capability in making a difference, cyber-physically, to its stakeholder's core values.

Information comes from a cyber user emerged on the priority to access services. Such information can be freshly generated, or (re-)presented from the existing information that has been used by the same cyber user elsewhere or from its physical human agent counterpart. To name a few, a brand new login ID created, an existing email ID provided for identification or verification outside of the email service provider; residential address, mobile phone number, date of birth, and/or security questions and answers, etc. personal information from physical world as part of the identification information. Such information has cyber-physical inputs to core values. This section studies causations of these inputs from cyber-user-generated information.

5.1 Freshly Generated Information

This cluster concerns information freshly generated by cyber-users that will create or enhance a difference to the user's CVs. For example, information of a new user name is self-centric to create or enhance a difference for the service provider to distinguish the user the user name represents from other users. It also makes a difference for the known status to the existence of the cyber agent that drives the user, from outside of the service's coverage to be included within. A further difference, inevitably made to the known status of the cyber behavior of the user is its human agent counterpart's mental status - in the first place, is a cyber experience. The difference made to the human agent includes the known status on its physical mental status in which influenced by its cyber behaviors. E.g., information generated by an online flight price comparison makes a difference on the user's known status about the counterpart human agent's travel plan behavior. Such a difference can lead to those who obtained the information to reassess their trust and respect towards the human agent, and can accordingly adapt resources within their availability for the human agent to access - such

evolution, when view the human agent as an independent individual, *can* make a difference on the human agent's CVs, among which the most affecting ones are: dignity (reflected by existence known status, identifiable probabilities) leading to trust and respect, opportunities (that implies resource accessibility) and ability (to develop the self from available resource) - all can lead to evolutions in the security and privacy dimensions.

Remark:

1. Information-as-a-difference in this cluster remarks *existence* of its creator - the associated cyber agent, its connection to the service provider and the human agent counterpart:
    - From the cyber agent's perspective, existence as a user of a service means the ability to access the service as (new) available resource. It also means more information about the cyber user for *others* to know about its existence and thus more opportunity to be *accessed* by others.
    - From the human agent counterpart's perspective, existence as a cyber user means the ability to obtain more cyber experience, and obtain the service resource without physical restrictions like time and location, physical identification (but through anonymity or pseudonymity, when applicable), or physical presentation. It also means more information about the physical self for others to access via its cyber counterpart[1].
    - From an external agent's perspective[2], a new existence comes into the world in which it lives means new knowledge about the existence and new opportunity to access to the existence's resource[3].
2. This cluster of differences reflects information's
    - *social paradox* in core values *resource* (enabling access) vs. *privacy* (constraining known status to existence)
    - *cyber-physical paradox* in core values cyber-*ability* (cyber enabling as an extension to physical ability) vs. physical-*ability* (physical constraining self-control of access to information about the self and the physical self).

5.2 Existing Information Presented

This cluster concerns existing information presented from one repository to another, without changing its content and presentation. Cyber repository of user-generated information is largely reserved by service provider. E.g., an email ID obtained from one service provider is presented to another as part of the user's profile to gain access to the service. When the information is presented from the existing information, it makes a difference to *usability* of the information and the known status to the *existence of the entity* the information represents - e.g., an email ID can be used for verification to access other services, and the existence of the email account is known to a wider extent that is extended to include the new service's coverage. A series of subsequent differences *can* follow:

- Purpose of the information

  When the purpose of the presentation not aligning with the information stakeholder's expectation about the information's existence, a difference will be made to the information's existence purpose. E.g., presenting an organization's name as one's affiliation while one is not affiliated with the organization.

---

[1] Such an access can be from cyber to physical, or from physical-cyber to cyber-physical; and then from physical to physical.
[2] "External" is by comparative to the integrity of cyber agent and its human agent counterpart.
[3] It can also mean lesser resource available to access from the shared service but here we focus on the difference the information made to its stakeholder.

- Integrity of the information

  Presenting a portion of the information that was created to exist as integrity[1] can make a difference to the conditions under which the information integrity is required. Such a difference can make a difference to the conditions' social dimensions (such as liability and rights) and associated core values (such as dignity, trust and respect).

- Right to the information

  A difference made to the information's existence purpose can adapt the stakeholder's ability to control the information towards his/her expectations and a subsequent difference to the stakeholder's right to control the information. A reset to security level of the information and/or associate security (such as financial security, job security, etc) will follow, stimulating a change of associated dignity, trust, respect towards the stakeholder.

- Access to opportunities

  A difference made to the right to control the information leads to a difference to the ability of accessing information, which can result in a value change of the information on its existing social influence, it makes a difference to the stakeholder's social availability (opportunities) to access the information value for developing desired social positions towards desired core values. E.g., as a result of inappropriate use of affiliation, one's right to information representing the affiliation is removed. This means one's access to opportunities associated with the organization is no longer available. All trust, respect and ability stimulated by the affiliation will follow to be adapted.

- Access to the self

  Differences to the information's repository and original purpose of existence make a difference to the usability and the action purpose of the information (Chen and Williams, 2011); together with a difference made to its stakeholder's right to control the information, make a difference to self's availability of being accessed - via or enhanced by the information being presented.

Remark:

1. Information-as-a-difference in this cluster remarks information's *existence, purpose, usability* and *integrity*; as well as its stakeholder's *existence status* (e.g., unknown, identifiable, anonymity, pseudonymity), *right to information* and *be-accessible status*.
2. This cluster of differences reflects information's
   - *social paradox* in core values i) *resource* (service) and *ability* (enabling access) vs. ii) *privacy* (constraining known status to existence) and *dignity* (constraining right to information and de-identification)
   - *cyber-physical paradox* in core values i) cyber-*ability* (cyber enabling as an extension to physical ability) vs. ii) physical-*ability* (constraining self-control of access to information about the self and the physical self).

[1] The notion of integrity of information is understood as an alignment of purpose of information and its usage (Chen and Williams 2010b). As the authors have observed, many types of information can be partitioned. Different parts of information can have different impacts on the stakeholder's core values.

5.3 Existing Information Re-presented

This cluster concerns existing information being re-presented differently, in structure, content, or repository, from its origin. Semantically,

- Being re-presented differently in structure means the *presentation* of the information is different from the original presentation. E.g., a picture is described in text, a story is described in different languages or different background (e.g., filter out partial context), a relationship is described by a metaphor, an organization is described as another organization's partner, a paper is presented in a different format, etc.
- Being re-presented differently in content means the information is presented differently in property dimensions like size, amount, volume, granularity, scope, and magnitude. I.e., the information is expressed in different dimensions to different degrees.
- Being re-presented differently in repository means the information is presented in a location different from where the information was acquired.

Re-presented information inherits information's capability in making differences form the cluster of Existing Information Presented (Section 5.2), i.e., information-as-a-difference to purpose, integrity, right, access and associated core values.

Remark:

1. Information-as-a-difference in this cluster remarks information's *existence, purpose, usability*, *scalability* and *integrity*; as well as information stakeholder's *existence status* (e.g., unknown, identifiable, anonymity, *pseudonym*), *right to information* and *be-accessible status*.
2. This cluster of differences reflects information's
   - *social paradox* in core values i) resource (service) and ability (access enabling) vs. ii) privacy of existence (known status constraining) and dignity (right to information and de-identification constraining)
   - *cyber-physical paradox* in core values i) cyber-*ability* (cyber enabling as an extension to physical ability) vs. ii) physical-*ability* (constraining self-control of access to information about the self and the physical self).

5.4 Summary

The three types of information can create three clusters of differences. While these differences all reflect information's paradoxical problem in core values "*resource/ability* vs. *privacy*" and "*cyber-ability* vs. *physical-ability*", each cluster of differences contributes to different affecting factors of privacy – namely, *access*, *right*, *integrity* and *purpose*.

6 PRIVACY CONSTRUCT

Through the studies above we have arrived at an understanding of key concepts that play important roles in understanding privacy status. These key concepts take effect in an integrity of CVs during information's existence. To facilitate privacy design for IS, based on the framework presented in Figure 1, we model these key concepts into privacy constructs in Figure 2.

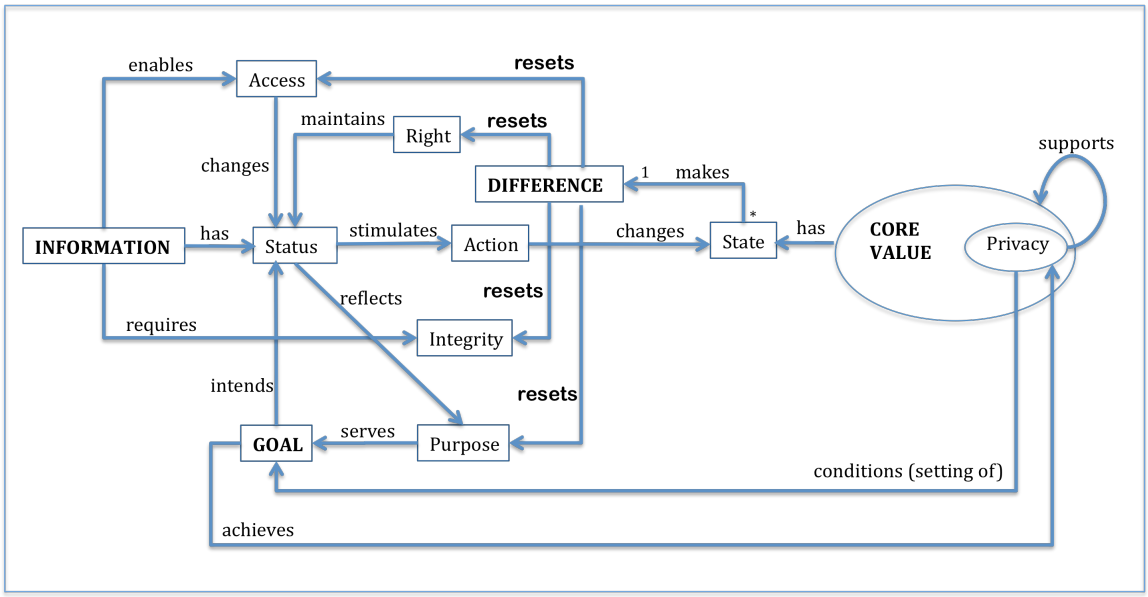

Figure 2. Privacy Construct

On interpreting Figure 2, we learn: information can stimulate actions (enabling or constraining) to change states of one's CVs. The Status of information is initially created by user actions based on the type of information (as described in Section 5), and later the difference made by the change of CV State can incur further changes via resets of Access, Right, Integrity and Purpose.

A state change of one CV can incur a state change of other CVs. State changes of CVs can make a difference to accessibility to the information and its stakeholder, his/her right to the information, intended purpose of the information existence, and the integrity status and conditions of the information. To achieve privacy (on the notion described in Section 2.1), the stakeholder establishes a set of goals to approximate intended status of the information towards a desired state of his/her CVs. The Core Value construct consists of 8 core values, namely *dignity*, *privacy*, *security*, *trust*, *respect*, *resource*, *ability* and *opportunity*. These values represent user's preference level.

The Difference construct is a place holder for reset types (i.e., Access, Right, Integrity or Purpose) and reset condition (i.e., the State of CVs). An important note to make is the creation of Goal needs to be conditioned by the existing CVs, e.g., ability and resource, to approximate the achievement within expected timeframes. This construct can be built on utilizing the Goal ontological grounds proposed in Chen and Williams (2010b).

7 CONCLUDING REMARKS

Privacy-by-design is an open issue in privacy-friendly information systems (Williams 2009; Chen and Williams 2010a, 2010b; Cavoukian 2010), meaning building privacy protection methodology into technology at the design phase. While "information" is a central element in information systems, there is a deficiency in addressing information's fundamental issue and models from a privacy management perspective - the core to privacy-by-design. This paper seeks to advance understanding of information's capability of making a difference to one's life, in particular, the aspects relevant to privacy status. These privacy relevant aspects are information purpose, integrity, privacy rights, access, core values (dignity, privacy, security, trust, respect, resource, ability and opportunity), and

goal. Based on these findings, a model of privacy construct is proposed to support privacy-by-design for information system development.

This research is a grounding study for understanding information's social feature and its impact on privacy within the CVF and the SRF. The privacy construct model (Figure 2) captures fundamental elements and information flows among them in making a difference to one's privacy. Therefore, while the primary target reader is system designers and developer, business and end-users can also benefit from learning the grounds of "information+privacy" in an IS context to better manage their information with privacy concerns.

The privacy construct model has the potential to be adapted into domain-specific information system for design with privacy concern for user-generated information. Future work will ground representations for the privacy construct model (Figure 2) and model user behaviors for robust collaborative information system development.

References

Bateson, G. (1972). Steps to an ecology of mind. New York: Ballantine Books, 1972.

BeVier, L. R. (1995). Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection, 4 WM. & MARY BILL RTS. J. 455, 458 (1995)

Cavoukian, A. (2010). Privacy-by-Design. Retrieved 22 April, 2010, from http://www.privacybydesign.ca/publications.htm

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). Privacy: An Ontological Problem. In *PACIS 2009 Proceedings.* Paper 134.

Collins, A. (2007). From h = logsn to conceptual framework: A short history of information. *History of Psychology* (10:1), pp.44-72.

France-Presse, A. (2007). Home trashed in myspace party. Retrieved 08 April, 2009, from http://www.news.com.au/story/0,23599,21549624-2,00.html

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

Moses, A. (2009). Social not-working: Facebook snitches cost jobs. Retrieved 08 April, 2009, from http://www.smh.com.au/articles/2009/04/08/1238869963400.html

Partridge, E. (1966). Origins: A short etymological dictionary of modern English (4th ed.). London: Routledge & Kegan Paul, 1966.

Shannon, C. E. (1948). A mathematical theory of communication. *Bell Systems Technical Journal*, 27:379-423 and 623-656, 1948.

Vodafone. (2011). Vodafone in privacy information leak. Retrieved 9 January, 2011, from http://au.news.yahoo.com/latest/a/-/latest/8615722