

Rethinking the Privacy and Identity Relationship

Richard Baskerville

*Department of Computer Information Systems
Georgia State University
Atlanta, Georgia 30303, USA
baskerville@acm.org*

Tawfig Alashoor and Ruilin Zhu

*Department of Computer Information Systems
Georgia State University
Atlanta, Georgia 30303, USA
{talashoor1 & rzhu} @gsu.edu*

INTRODUCTION

Much of the privacy literature takes a monolithic view of identity. This view associates a physical person (hereafter an “person”) with a single, perpetual identity. At its extreme, this monolithic view might be presented as:

$$\text{person} = \text{identity}$$

This view basically states that a person is their identity. It is one dimensional. While this view is culturally embedded in many of western societies, it is partly the source of many otherwise insurmountable problems with privacy protection. It requires in a modern society that a protecting person’s privacy necessarily involves the ultimate production of their identity. That is,

$$\text{privacy}(\text{person}) = \text{privacy}(\text{identity})$$

In this position paper, we suggest that there are new, additional privacy protection measure that arise with this monolithic relationship is reconsidered. For example, because of the monolithic view, the predominant approach to privacy protection is preventative, a security management style that is known as “left-of-bang” (Baskerville, Spagnoletti, & Kim, 2014). This terminology refers to an unwanted incident as a “bang”, and “left” refers to a timeline leading up to the incident (left to right). See Figure 1. The kind of management that is effective left-of-bang (predicated on detection, prediction, probability, etc.) is rather different in nature that that which is effective right-of-bang (predicated on agility, improvisation, possibility, etc.). For privacy compromises, right-of-bang remedial measures and recovery from loss are complex, ad hoc, and limited in effectiveness. Preventative measures are indeed paramount. However, we presently lack theoretical depth in the essential preparation for recovery in those severe cases where preventative measures fail.

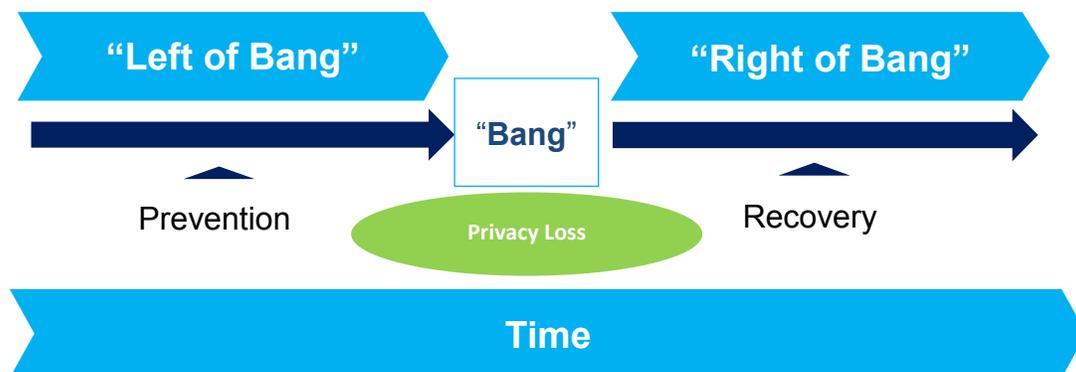


Figure 1. Privacy loss incident timeline

Theorizing in this area requires an essential rethinking of the monolithic view of the relationship between the person and their identity is a first step to rethinking how we can better manage accidental or intentional privacy exposures. Such a rethinking process should first question the basic monolithic assumption that an individual person has one, perpetual identity. Indeed, considerable research reveals that individuals have multiple identities of differing kinds.

SOCIALLY CONSTRUCTED IDENTITIES

A number of theorists in the early 20th century underscored the importance of identity for understanding human behaviors in particular and societies in general (Leary & Tangney, 2012). In the language of privacy discourse, the notion of identity becomes highly pertinent, merely due to the associated threat of privacy invasion to identity reconstruction. Yet to study privacy through the lens of identity is not an unchallenging task. It is evident that the identity literature encountered several waves of oscillations in that different researchers focused on various aspects of the identity concept (Schwartz, Luyckx, & Vignoles, 2011). This is due to the multifaceted nature of this concept (Brubaker & Cooper, 2000). For instance, identity contributes to explain many behavioral reactions in our lives whether these behaviors emerge from cultural, ethnic, or national differences (Baum, 2008; Moshman, 2007; Schwartz, Dunkel, & Waterman, 2009). It drives our life paths and decisions (Kroger, 2007). Identity also contributes to our sensible perception of strengths we draw from social and group affiliations (Brewer & Hewstone, 2004; Schildkraut, 2007). Therefore, identity has been used, in the different disciplines within the social science, to refer to different facets including people's internal meaning systems, attachments and traits drawn from group memberships, nationalism, or narrative interactions (Bamberg, 2006; Brown, 2000; Vignoles, Schwartz, & Luyckx, 2011; Schildkraut, 2007). The fuzziness of this concept has even led some scholars like Baumeister to believe that identity or the self "is not really a single topic at all, but rather an aggregate of loosely related subtopics" (as cited in Leary & Tangney, 2012, p. 1).

Nevertheless, we draw upon Vignoles et al.'s (2011, p. 2) succinct but comprehensive definition of identity which "involves people's explicit or implicit responses to the question: "Who are you?" This definition deals with many of the intricacies of the term *identity*. First, the "you" refers to both individual (singular) and group (plural), e.g., "I am an American" and "We are Americans." Second, the "Who are you?" can be used reflexively, such as "Who am I?" and "Who are we?" Yet this reflexive question not only encompasses "who you think you are," – either in singular or plural form - but also "who you act as being" in interpersonal and intergroup communications (Vignoles et al., 2011, p. 2). Therefore, this definition of identity comprises and pertains to a number of contents and processes that are diverse but also related to each other (Vignoles et al., 2011).

According to the literature, there are three - individual, relational, and collective - levels through which identity is defined (Sedikides & Brewer, 2001). Individual identity, which also refers to personal identity, is defined as "aspects of self-definition at the level of individual person," such as goals, values, and beliefs (Vignoles et al., 2011, p. 3). Relational identity refers to the roles of a person in relation to other people, including identity contents, e.g., parent, spouse, customer, etc. (Vignoles et al., 2011). Yet, relational identity is also pertinent to how these roles are defined and perceived by the individuals who assume them (Vignoles et al., 2011). In this context, many social scientists maintain that identity is defined and found within

interpersonal space (Bamberg, 2004), families (Manzi, Vignoles, Regalia, & Scabini, 2006), or a larger structure (Thatcher & Zhu, 2006). Hence, an identity cannot be established by an individual in his or her own (Vignoles et al., 2011), in that it needs to be recognized by the society (Swann, 2005). This claim unfolds that identity is de facto socially constructed. Finally, collective identity simply refers to “membership of any kind of social group” such as ethnicity, nationality, gender, families, etc. (Vignoles et al., 2011, p. 3). It is also emphasized that individuals can have material identities in that individuals view and treat material artifacts, such as house, clothes, cars, contents of a bank account, as part of their identities (Vignoles et al., 2011).

A. Polymorphism

According to the above discussion, multiple identities do exist within one individual or a group of individuals (Vignoles et al., 2011). For instance, one person can be Christian, a social scientist, American citizen, and an owner of a bank account. These multiple identities become more or less distinct depending on the context or setting (Vignoles et al., 2011). However, they are not independent of each other but they interact with each other (Amiot, de la Sablonnière, Terry, & Smith, 2007). Moreover, the fact that “possible identities” is an area of study among social scientists reveals the polymorphic of one’s identity. Possible identities, as part of the future self, are working philosophies of who one may become in the future based on self-assessments of personal strengths, weaknesses, talents, and characteristics (Oyserman & James, 2011). According to the literature, possible identities have been studied within four main areas: life phases and transitions, socio-demographics, identity valence and balance, and identity distance (Oyserman & James, 2011). Thus, polymorphism is a focal characteristic of identity.

B. Socially Constructed

With regard to the construction of identity, one should view identity through “the definitions and meanings of identity categories as ideas in their own right” (Vignoles et al., 2011, p. 4). Identity categories, in any cultural milieu and historical times, have specific definitions and meanings that have been socially established and constructed (Vignoles et al., 2011). In addition, identity categories maybe mooted, deconstructed (Vignoles et al., 2011), or even reconstructed. Subsequently, identity is viewed through ways of thinking/talking that appear to be salient in a specific social and historical context, yet independently of any one individual (Rattansi & Phoenix, 2005) because they are constructed through a concourse of social processes over the history (Burkitt, 2004).

C. Artificial

Identities have different meanings in different times due to the historical and social construction influences. Moreover, identity is characterized by its polymorphic nature. These assumptions entail the artificiality of the identity establishment because one’s identity is devised differently depending on the cultural milieu, historical times (Vignoles et al., 2011), or one’s assessments of self-characteristics (Oyserman & James, 2011). Hence, artificiality becomes another focal characteristic of identity.

Attributes

In the digital world, however, the identity or what henceforward we may refer to as “online identity” of an individual encompasses various but related attributes. To simply categorize such attributes, three main aspects, namely possession, capability, and distinction, maybe exhaustive. First, the online identity has the ability to possess materials, e.g., money in the bank account that is seen as intangible but usable currency. In this case, the online identity, which may be defined by user name, password, token, fingerprint, etc., plays an

important role in managing this account. Thus, online identity is actually capable of carrying out operations, e.g., managing bank account, placing a purchase order on Amazon, contacting customer service, interacting with other people or “other online identities” on Facebook, etc. The notion of capability leads to thinking of or looking at the online identity as a metaphor of personal identity. This cannot be true unless one online identity can be distinguished from other online identities. Thus, distinction, such as IP address, Gmail account, Twitter account¹, etc., is another focal attribute of the online identity.

D. Onion Skin Model of Identity

According to the above discussion, identity, per se, is a multifaceted concept, and individuals’ identities become more sophisticated when considering the advanced information and communication technologies (ICTs) as new identities continue developing. Therefore, we propose a collection of identities using an onion skin model after considering the notion of integrative identity suggested by (Vignoles et al., 2011) and apply it into the digital world. We succinctly limit our model to a number of identities, namely, personal identity, social identity, online identity, and digital identity. Although this collection of identities is abstracted considering the minutia of fragmented identities, they are eminently linked to the notion of privacy in the digital world. This implies that future studies may expand on this proposed model by including other facets of identity. More importantly, the implications of using an integrative identity when studying the impact of the digital world will enrich our understanding of the digital privacy. Yet this is not the main scope of this manuscript.

Personal Identity

Personal identity is “the individual self which is associated with close personal relationships and idiosyncratic attributes of the person” (Leary & Tangney, 2012, p. 503). Personal identity is also related to the concept of existence as someone might think “Who am I? Am I going to have another life after death?” (Korfmacher, 2014). This definition captures one aspect of the detailed discussion of identity definition in the previous section (Vignoles et al., 2011). Nevertheless, John Locke’s view of personal identity is about consciousness where neither the body substance nor the soul is dependent on the identity. The notion of personal identity or the self is still ambiguous even with the extant copious literature. The implicit meaning and philosophical perspective could be one of the reasons this concept is difficult to be discerned. However, in our daily lives, we may perceive personal identity through a collection of attributes such as name, age, or appearance. These attributes reflect the idiosyncratic attributes mentioned in Leary and Tangney’s (2012) definition of personal identity. It is worth to mention that personal knowledge is viewed as the personal privacy (Baskerville & Dulipovici, 2006) and an individual attribute part of personality (Dulipovici & Baskerville 2007), and therefore it can be included as another attribute personal identity. Citizenship and race can also be seen as attributes of a single person but they actually are socially constructed, as explained by Vignoles et al., 2011 that personal identity and social identity cannot be disentangled.

Social Identity

According to Tajfel (1972), social identity is “the individual’s knowledge that he belongs to certain social groups together with some emotional and value significance to him of his group membership” (as cited in Leary & Tangney, 2012, p. 502). This definition institutionalized the social identity theory which has been tremendously used to study group processes, collective self, group membership, and intergroup relations. In

¹ Examples given such as Gmail and Twitter accounts should be thought of Gmail unique user ID.

sociology, symbolic interactionism proposes that focusing on the individual person regardless of the social structure, or vice versa, is partial and insufficient (Blumer, 1937). According to Ellsworth Faris (1937) and Herbert Blumer (1937), symbolic interactionism refers to “the meaning of things - including the self - is derived from social interaction, the reactions of significant others, and one’s interpretation of those interactions” (as cited in Leary & Tangney, 2012, p. 2). In this sense, reality as well as identity is socially constructed. The social structural context plays a critical role in shaping identity (Stryker, 2003). Put simply, “identities are inescapable both personal and social not only in their content, but also in the processes by which they are formed, maintained, and changed over time” (Vignoles et al., 2011, p. 5).

Online Identity

While there is no consensus among scholars regarding the distinction between online identity and digital identity, we propose that online identity can be distinguished from digital identity. Online identity is a social identity that is constructed through online interactions and communities but not offline ones. Nabeth (2005) defines online identity in a similar way yet uses the term interchangeably with digital identity. Charney (2009), on the other hand, uses online identity to refer to what we discuss below as a digital identity.

Internet users communicate with each other for several purposes, such interactions can be seen as social interactions but in a digital format. For example, an individual joins an online community that is interested in games. This person may or may not use his or her real personal identity or social identity. This person could use pseudonyms and personal attributes that are not true to him or her “personal identity.” Also, this person could reform his or her social identity in order to build a blended social identity that would fit the new online society “social identity.” Therefore, this person may build an online identity using a new personal and social identity, deriving it either from his or her real personal and social identities or based on the new online milieu, or constructing it by synthesizing both real and new identities since a person in the online social relationship tends to misrepresent himself than in offline relationship (Baskerville & Sainsbury 2006). On the one hand, when a new personal and social identity is constructed, privacy threats are not very crucial because they do not form a threat to the real personal and social identity. However, this is rarely the case compared to individuals who use their real personal and social identities in the digital world. On the other hand, when using real or a blend of real and new identities, privacy threats become very critical as they bring about a threat to the real personal and social identity.

Digital Identity

Digital identity is pertinent to the data that uniquely define a person and his or her relationship to other people (Windley, 2005). According to this definition, one can recognize that the digital identity, e.g., IP, Facebook, Google+, or Twitter, is a very strong indicator of the online identity. For instance, a record of an individual in the unmeasurable database owned by Facebook maybe comprised of several attributes pertinent to him or her. Even though some attributes may correlate with the social structure, in this case, they belong to the individual him or her –self. Therefore, by assuming that the online identity is more related to social identity than personal identity, in this sense, identity theft is pertinent to the digital identity but not the online identity, as it uniquely identifies the attributes required to seize a personal identity.

Once again, if the online identity was constructed using unreal personal and social identity, privacy is not a big matter. However, if the online identity is a metaphor indicating an individual’s real life and real social interactions, privacy invasions are very consequential. Hence, a threat to the digital identity brings about a threat to online identity; and if true personal identity and social identity were used to construct the online

identity, a threat to the online identity generates a threat to the social identity and the personal identity, respectively. The threats to the social and personal identities are hypersensitive as they are directly related to the physical milieu.

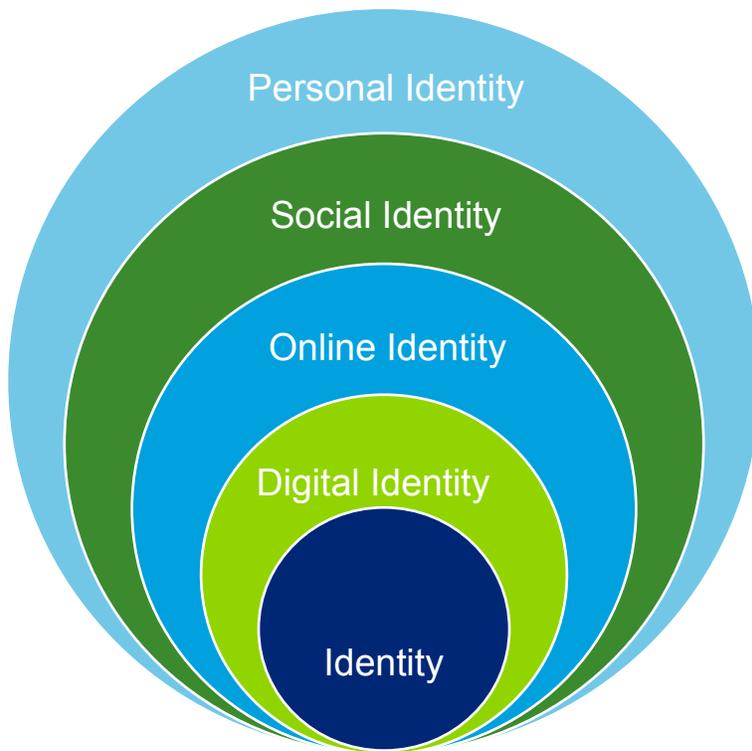


Figure 2. Onion-like socially constructed identities

E. Physical Identity

Recognizing that an individual person is already associated with multiple forms of identity may be arresting for some readers. However, none of the socially constructed forms of identity described above account for the physical identity of the individual person. The physical identity of an individual may be viewed as the information associated with the corporal body of that individual. For most identity management systems (Millett & Kent, 2003), the overarching task of which is to determine whether an individual's claimed identity in its socially constructed sense matches their physical identity in terms of the physical hair, eye color, fingerprints, retina or iris patterns, facial geometry, height, weight, etc.

With the mounting need of the verification of an individual's identity, several methods have been brought forward, and implemented: from "what s/he possesses" (e.g., an ID card) or "what s/he remembers" (e.g., a password) to "who s/he is", which refers to *biometrics* (A. Jain, Bolle, & Pankanti, 1996). Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person (A. K. Jain, Flynn, & Ross, 2007). Compared to other systems, it is able to offer certain unique advantages such as negative recognition and non-repudiation (Prabhakar, Pankanti, & Jain, 2003). In addition, biometrics cannot be easily stolen or shared, and it is also convenient to use without bringing the ID card or remembering passwords.

Due to its effectiveness and convenience, biometrics has been utilised for identification and authentication (Clarke, 2001) in law enforcement (e.g., illegal aliens, security clearance for employees for sensitive jobs, fatherhood determination, and forensics), and also is being increasingly used today to establish person recognition in a large number of civilian applications (A. K. Jain, Ross, & Prabhakar, 2004) and socialization (e.g., fingerprint password for mobile phone and laptop, facial recognition in Online Social Networks).

An individual's identity that is being determined by biometrics, or biometric identity, therefore, might soon be perceived as the primary and single identity (de Andrade, Martin, & Monteleone, 2013). As it contains the unique nature of biometric data of mainly physical attributes of an individual, we view it as the *physical identity*.

An attribute can be used as physical identity as long as it satisfies the following requirements: universality, distinctiveness, permanence, and collectability (Prabhakar et al., 2003). While *universality* means that almost every individual should have this physical attribute, *distinctiveness* suggests that each should have noticeable differences in the attribute. *Permanence* refers to the feature that the attribute should not change significantly over time, and *collectability* relates to the characteristic that it should be effectively determined and quantified.

The attributes that are widely adopted for physical identity include fingerprint, facial image, hand geometry, iris, retina, palm-print, ear/wrist/hand vein, or the DNA information (Chandrasekaran, 1997; James, 1997; Wayman, Jain, Maltoni, & Maio, 2005; Woodward, 1997).

One example for the physical identity is the wide use of e-passport. Many countries have started issuing e-passports to the holder with an embedded chip holding an individual's physical identity of biometric data, such as facial image, fingerprint, since 2006 (Hoepman, Hubbers, Jacobs, Oostdijk, & Schreur, 2006). It has improved the efficiency of border control and effectively addressed the security concerns over the illegal immigrants or terrorists (Häkli, 2007).

India is the first large country in the world to implement the physical identity scheme at an unprecedented scale of Unique Identification Authority of India (UIDAI), which has chosen to use facial image, iris, and 10-print fingerprint rather than a physical ID card (Ricanek Jr, 2011). By 2014 half of India's population will have registered in UIDAI (Rai, 2012), enabling the previously anonymous poor Indians to get access to services such as bank accounts, and driving licenses.

Physical identity, however, has certain limitations (O'Gorman, 2003). Facial image and voice are obviously not secret, which can be captured by taking a photo or a recording, and it is difficult to keep a fingerprint secret as an individual may touch or hold some article, which can be effectively collected as well. Moreover once the physical identity is compromised, it cannot be easily replaced.

Like personal identities (socially constructed identities), physical identities encompasses similar attributes: possession, capability, and distinction. First, the physical identity has the ability to possess materials, e.g., gold or cash money that is seen as tangible currency. In this case, the physical identity is physically associated with such material. Likewise, the physical identity has various capabilities with physical possessions. Such possessions can be physically operated by transfer or trade. Likewise there are physical distinctions such as the aforementioned physical hair, eye color, fingerprints, retina or iris patterns, facial

geometry, height, weight, etc., which may be defined by user name, password, token, fingerprint, etc., plays an important role in managing this account.

F. Identity bridges

If we admit that there can be (and indeed already exist) multiple types of identity, then our original monolithic view of identity, then our original conception of a person's relationship to their identities becomes conditions on which type of identity is under consideration (physical, digital, online, etc.). We might represent such

$$\text{person} = \text{identity}(\text{person}, \text{identity type})$$

The above reformulation states that, for our purposes in privacy, a person is made up of different types of identity. This is a two dimensional reformulation of identity. Our privacy formulation then becomes:

$$\text{privacy}(\text{person}) = \text{privacy}(\text{identity}(\text{person}, \text{identity type}))$$

These varying types of identity, physical identity and the various socially constructed identities are connected in various specific ways. The socially constructed identities are nested. But these are collectively connected with the physical identity, most often in a singular way. Most apparently, we can regard the connection of the physical identity to the various kinds of social identity as a *bridge*. In societies that regard identity as sharing a monolithic, perpetual relationship with the person presume that this bridge is also perpetual. Many of the most problematic privacy protection concerns involve crossing (or preventing others from crossing) the identity bridge between physical identity and other kinds of identities.

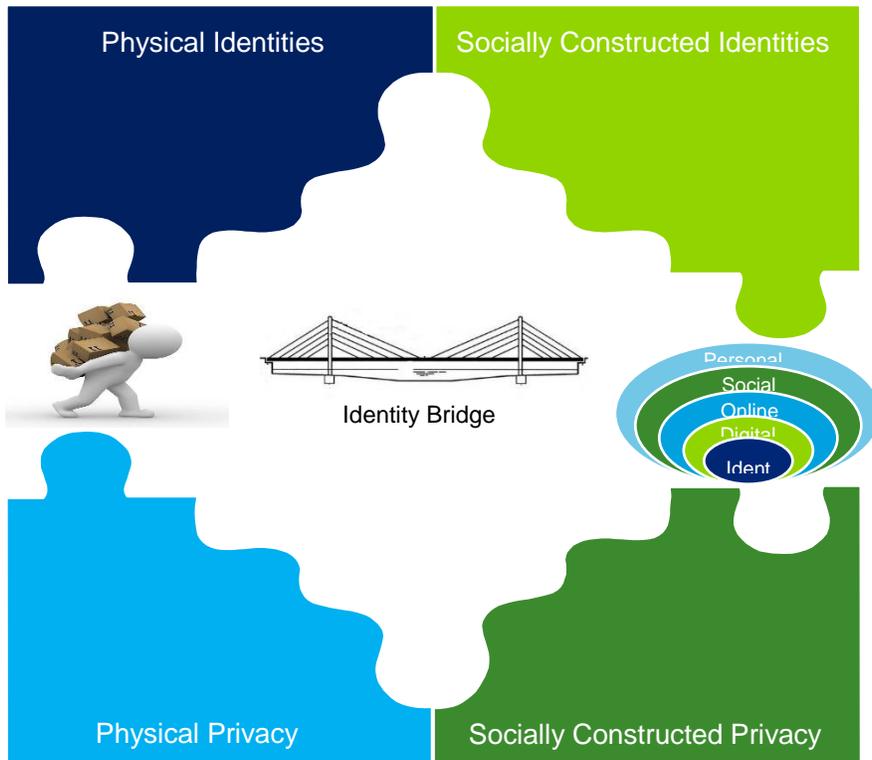


Figure 3. Identity Bridge

The privacy breach can happen on *either* side of the identity bridge, which however leads to distinct consequences on the *other* side. We will briefly discuss about each case and its implications.

Case I Breach on Physical Identity

Physical identity can be breached due to the nature of biometric data as aforementioned. Attacker can get access to some crucial biometric attributes, such as fingerprint, facial image, by simply taking fingerprint powder or photos, or by directly hacking the fingerprint database which store the information for attendance, for instance. With the wide use of physical identity as the primary authentication method for sensitive personal belongings in lieu of password, such as laptop, mobile phone, the attacker theoretically will be able to obtain more sensitive data that are stored at these devices. In this regard, breach on physical identity will lead to the loss of socially constructed privacy that is established by other kinds of identities on the right side.

Case II Breach on Socially Constructed Identity

Under certain circumstance, the socially constructed identity can be infringed. For example, a user's personal information, such as his hometown, education background, working history, travelling records, can be constantly collected from his posts at Online Social Networks (we assume him is an active user). With the trace of the bit and bit information, the paparazzo may eventually identify who the user really is, which further enable the possibility of knowing more facts about the user, like his preference, geographic locations, destroying the anonymity that lies in the core of physical privacy. In this sense, the infringement on socially constructed identity will result in not only the breach of other kinds of identities on the right side, but also even the physical identity that crosses the bridge on the left side.

In conclusion, the physical identity and the various socially constructed identities are connected by the identity bridge in specific ways. While it suggests the close relationship between them, it also emphasizes the possibility that by crossing the bridge, the attacker is able to breach the identity to erode the privacy on the other side with the available information on one side.

MANAGING IDENTITY

The particular role of the identity bridge provides a possibility of right-of-bang recovery by increasing our ability to manage the identities associated with each individual person. We can consider the primitive operations that might be available for managing identities. Given the onion-like nature of identities, a series of managerial operations can be applied to them, viz. read/write, create/delete, and associate/disassociate.

Read/Write: an individual has layers of identities, which can be accessed to by authorised request from identity administrator. This kind of request is able to add some new information to the existing identity as *write* or obtain the information as *read* upon the demand of its owner or administrator.

Create/Delete: this pair of operations involves the process of building new layer(s) of identities or destroying the old one(s). Under certain situation, an identity for a specific individual can be established as *create* by adding the necessary attributes that is relevant to that identity onto the designated layer of identity or be demolished as *delete* by remove all necessary record from a certain layer.

Associate/Disassociate: facilitated by these operations above, the socially constructed identities can be effectively connect or disconnect with the physical identity of an individual. Once the individual finds the need of incorporating new established identity(ies) to his physical identity, it can be achieved by doing connection operation as *associate*, while he feels the necessity of abandoning the existing identity(ies), it can also be executed by conducting disconnection operation as *disassociate*.

By enabling these operations, we achieve more flexibility, perhaps even agility, in managing socially constructed identities as well as physical identity. Such fundamental operations open ways to recover from incidents right-of-bang, and therefore add more secure protection (recovery protection) to improve individual privacy.

A. Reconsidering the cultural properties of identity

In most developed economies, the notion of opening a bank account with a different name than last time is culturally regarded as suspicious behavior. For a moment, suspend this suspicion and consider an alternative culture.

In certain Native American cultures, a physical person may have multiple identities over their lifetime. At birth, parents might give their baby its true name. For example, imagine a child given a true name of *Towanda*. This name may sometimes only ever be known to the parents and Towanda. The tribe will name the child on some other basis. For example, if Towanda is small, attractive and smells nice, the tribe may name the child *Little Flower*. Entering teenage years, the tribe might collectively decide that Little Flower is gone, and based on Little Flower's more recent nature, rename the child *Angry Goat*. But as Angry Goat matures in adulthood, and becomes an accomplished achiever and respected member of the tribe, the tribe might realize that Angry Goat is no more, and name this adult *Soaring Bird*. Later, Soaring Bird might be replaced by *Wise Eagle*, and so-on. It may be, after all, that Wise Eagle is the only person who knows anything about Towanda.

In such a tribal society, these are not just different names for the same person. These are different persons with different identities as time moves on. Such a tradition may provide a key for coping with recovery-style, right-of-bang privacy protection in a society that nests each individual person's identity in networks with thousands of computers. For Towanda, identity changes over time. We might represent this evolution as

$$\text{person} = \text{identity}(\text{person}, \text{identity type}, \text{time})$$

The above reformulation states that, for our purposes in privacy, a person is made up of different types of identity, each of which may be different at different points in time. This is a three dimensional reformulation of identity. Our privacy formulation then becomes:

$$\text{privacy}(\text{person}) = \text{privacy}(\text{identity}(\text{person}, \text{identity type}, \text{time}))$$

B. Implications: Preparing Identity Recovery

The implications of this reconceptualization of the identity that privacy seeks to protect could be profound. Because identity is a polymorphic social construction that emerges, extending such an identity with a disposal privacy layer is feasible. Consider this vignette.

Juhani Peltoniemi, resides at 23B Sauna Street in Copperwood Michigan. Juhani opens a bank account at the Copperwood Bank. Together Juhani and the bank create an identity for Juhani named John Brown. This

identity, John Brown, is associated with a distinct person id number, and *attributes* (such as a credit history) that are equivalent to (but not exactly the same as) Juhani's. These attributes are John Brown's, not Juhani's.

Such an added identity would effectively create a new outer layer in the identity onion. We may call this a *hide*, both a tough, protective, outer skin, and an effective concealment for Juhani. Juhani and John might live at the same address. John has a Copperwood credit card, Juhani does not.

Let us suppose that the Copperwood Bank is hacked and totally compromised. John Brown's identity, banking records, and credit card number are stolen. The identity hide enables a different form right-of-bang recovery. Juhani and the bank create a new identity, Ian Green, different from both John and Juhani, but with equivalent (not exactly the same) attributes. Effectively John Brown moves away from 23B Sauna Street in Copperwood Michigan, and Ian Green moves in (with his bank account and credit card). A new identity hide is created, and the old one is deleted.

Preventing the compromise of John Brown's privacy from cascading to Juhani and Ian may be an issue of preventing "bridge crossing". Maintaining Juhani's privacy after John is compromised means preventing intruders from crossing the identity bridge to Juhani's physical identity. Re-crossing the bridge back to Ian's identity would be a further cascading compromise. Protecting a compromise of an identity hide from cascading to an individual's other identities is essential. Currently an important vehicle for access control is three layered: Something the user is, has, and knows (an attribute, a possession, a capability). It also depends on crossing the bridge between the physical and socially constructed identities. Use of this security mechanism itself needs rethinking because of its potential as a fundamental identity compromise.

FUTURE RESEARCH

Principles for Managing Polymorphic Identities

Such a rethinking of the role of identities in enhancing privacy protection in a network world raises many research questions that can be expressed as design principles for a polymorphic identity solution to privacy compromise recovery.

1. Legitimizing polymorphic identities
Current mores, laws, and regulations regard an individual person with multiple identities as suspicious. Such structures effectively prevent any form of *identity backup*; backup being one of the most essential information security mechanisms when right-of-bang recovery is needed.
2. Protecting identity bridges
Current practices frequently cross the identity bridge between the physical identity and the socially constructed identities. Protecting this bridge is essential for protecting any form of compromise on either side of this bridge from cascading across.
3. Regulating polymorphic identities
As well as regulating privacy, the state would take have a far more complex role in the governance of identities of its citizens and other individual persons. In order to protect the public by piercing identity hides, a package enforcement, including regulations, laws, framework, and standards, will be needed (Baskerville & McPherson 2009).
4. Deploying polymorphic identities

The deployment of polymorphic identities to the critical controlling societal services is the next step that is towards the comprehensive privacy protection. The service should be enabled at financial institutions, educational institutions, government organizations, etc.

5. Implementing polymorphic identities

The administrative organization should also be established to implement polymorphic identities from the top to the bottom across the society.

The monolithic view of a single, perpetual identity is becoming questionable due to the wide and grave concern over privacy protection. Rather than assuming that identity consists of only one dimension, we must accept the possibility that it may have three dimensions crossing from physical identity to socially constructed identities, which are connected by the identity bridge as we call. This structure theoretically enables the introduction and utilization of the polymorphic identity as one of the most effective mechanisms to recover from a privacy breach, which motivates a further in-depth institutional and academic research and exploration.

REFERENCES

- Amiot, C. E., de la Sablonnière, R., Terry, D. J., & Smith, J. R. (2007). Integration of social identities in the self: Toward a cognitive-developmental model. *Personality and Social Psychology Review*, 11(4), 364–388.
- Bamberg, M. (2004). Talk, small stories, and adolescent identities. *Human Development*, 47(6), 366–369.
- Bamberg, M. (2006). Stories, big or small: Why do we care? *Narrative Inquiry*, 16(1), 139–147.
- Baskerville, R., & Dulipovici, A. (2006). The ethics of knowledge transfers and conversions: property or privacy rights? In R. H. Sprague (Ed.), *Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS-39)* (pp. 144, CD-ROM 141-149). Los Alamitos, Calif: IEEE Computer Society.
- Baskerville, R., & McPherson, E. (2009). Security and Privacy Convergence: A Global Governance Perspective *Cutter IT Journal*, 22(8), 19-23.
- Baskerville, R., & Sainsbury, R. (2006). Distrusting Online: Social Deviance in Virtual Teamwork. In R. H. Sprague (Ed.), *Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS-39)* (pp. 121, CD-ROM 121-129). Los Alamitos, Calif: IEEE Computer Society.
- Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-centered information security: Managing a strategic balance between prevention and response. *Information & Management*, 51(1), 138-151.
- Baum, S. K. (2008). *The psychology of genocide: Perpetrators, bystanders, and rescuers*. Cambridge, UK: Cambridge University Press.
- Blumer, H. (1937). Social psychology. In E. P. Schmidt (Ed.), *Man and society* (pp. 144–198). Englewood Cliffs, NJ: Prentice-Hall.
- Brewer, M. B., Hewstone, M. (Eds.). (2004). *Applied social psychology: Perspectives on social psychology*. Malden, MA: Blackwell.
- Brown, R. (2000). Social identity theory: Past achievements, current problems, and future challenges. *European Journal of Social Psychology*, 30(6), 745–778.
- Brubaker, R., & Cooper, F. (2000). Beyond “identity”. *Theory and Society*, 29(1), 1–47.
- Burkitt, I. (2004). The time and space of everyday life. *Cultural Studies*, 18(2–3), 211–227.
- Chandrasekaran, R. (1997). Brave New Whorl: ID Systems Using the Human Body Are Here, but Privacy Issues Persist, *Washington Post*, p. 30.
- Charney, S. (2009). The evolution of online identity. *IEEE Security & Privacy Magazine*, 7(5), 56-59.
- Clarke, R. (2001). Person location and person tracking-Technologies, risks and policy implications. *Information Technology & People*, 14(2), 206-231.
- de Andrade, N. N. G., Martin, A., & Monteleone, S. (2013). All the better to see you with, my dear: Facial recognition and privacy in online social networks. *IEEE security & privacy*, 11(3), 21-28.
- Dulipovici, A., & Baskerville, R. (2007). Conflicts between privacy and property: The discourse in personal and organizational knowledge. *Journal of Strategic Information Systems*, 16(2), 187-213.
- Faris, E. (1937). *The nature of human nature*. New York: McGraw-Hill.
- Häkli, J. (2007). Biometric identities. *Progress in Human Geography*, 31(2), 139-141.
- Hoepman, J.-H., Hubbers, E., Jacobs, B., Oostdijk, M., & Schreur, R. W. (2006). Crossing borders: Security and privacy issues of the european e-passport *Advances in Information and Computer Security* (pp. 152-167): Springer.

- Jain, A. K., Flynn, P., & Ross, A. A. (2007). *Handbook of biometrics*: Springer.
- Jain, A. K., Ross, A., & Prabhakar, S. (2004). An introduction to biometric recognition. *Circuits and Systems for Video Technology, IEEE Transactions on*, 14(1), 4-20.
- Jain, A., Bolle, R., & Pankanti, S. (1996). Introduction to biometrics *Biometrics* (pp. 1-41): Springer.
- James, F. (1997). Body scans could make ID process truly personal. *Chicago Tribune*, June, 4, 1997.
- Kroger, J. (2007). *Identity: The balance between self and other*. London: Routledge.
- Leary, M. R., & Tangney, J. P. (2012). The self as an organizing construct in the behavioral and social sciences. In M. R. Leary, & J. P. Tangney (Eds.). *Handbook of self and identity*. New York: Guilford Press.
- Manzi, C., Vignoles, V. L., Regalia, C., & Scabini, E. (2006). Cohesion and enmeshment revisited: Differentiation, identity, and well-being in two European cultures. *Journal of Marriage and Family*, 68(3), 673–689.
- Millett, L. I., & Kent, S. T. (2003). *Who Goes There? Authentication Through the Lens of Privacy*: National Academies Press.
- Moshman, D. (2007). Us and them: Identity and genocide. *Identity: An International Journal of Theory and Research*, 7(2), 115–135.
- Nabeth, T. (2005). Understanding the identity concept in the context of digital social environments.
- O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12), 2021-2040.
- Oyserman, D., & James, L. (2011). Possible identities *Handbook of identity theory and research* (pp. 117-145): Springer.
- Prabhakar, S., Pankanti, S., & Jain, A. K. (2003). Biometric recognition: Security and privacy concerns. *IEEE security & privacy*, 1(2), 33-42.
- Rai, S. (2012). Why India's identity scheme is groundbreaking. *BBC News*, 6.
- Rattansi, A., & Phoenix, A. (2005). Rethinking youth identities: Modernist and postmodernist frameworks. *Identity: An International Journal of Theory and Research*, 5(2), 97–123.
- Ricanek Jr, K. (2011). Dissecting the human identity. *Computer*, 44(1), 0096-0097.
- Schildkraut, D. J. (2007). Defining American identity in the twenty-first century: How much “there” is there? *The Journal of Politics*, 69(3), 597–615.
- Schwartz, S. J. (2001). The evolution of Eriksonian and neo-Eriksonian identity theory and research: A review and integration. *Identity: An International Journal of Theory and Research*, 1(1), 7–58.
- Schwartz, S. J., Dunkel, C. S., & Waterman, A. S. (2009). Terrorism: An identity theory perspective. *Studies in Conflict and Terrorism*, 32(6), 537–559.
- Schwartz, S. J., Luyckx, K., & Vignoles, V. L. (2011). *Handbook of identity theory and research*. New York, NY: Springer New York.
- Sedikides, C., & Brewer, M. B. (2001). *Individual self, relational self, collective self*. Philadelphia: Psychology Press.
- Stryker, S. (2003). Whither symbolic interaction? Reflections on a personal odyssey. *Symbolic Interaction*, 26(1), 95–109.
- Swann, W. B., Jr. (2005). The self and identity negotiation. *Interaction Studies*, 6(1), 69–83.

- Thatcher, S. M., & Zhu, X. (2006). Changing identities in a changing workplace: Identification, identity enactment, self-verification, and telecommuting. *Academy of Management Review*, 31(4), 1076-1088.
- Vignoles, V. L., Schwartz, S. J., & Luyckx, K. (2011). Introduction: Toward an integrative view of identity. In S. J. Schwartz, K. Luyckx, & V. L. Vignoles (Eds.), *Handbook of identity theory and research*. New York, NY: Springer New York.
- Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (2005). *Biometric systems: technology, design and performance evaluation*: Springer.
- Windley, P. J. (2005). *Digital identity*. Sebastopol, CA: O'Reilly.
- Woodward, J. D. (1997). Biometrics: Privacy's foe or privacy's friend? *Proceedings of the IEEE*, 85(9), 1480-1492.