Privacy and Identity Theft Recovery Planning: An Onion Skin Model

Tawfiq Alashoor
Georgia State University
talashoor1@gsu.edu

Richard Baskerville
Georgia State University
baskerville@acm.org

Ruolin Zhu
The University of Auckland
ruilin.zhu@auckland.ac.nz

Abstract
Identity protection is currently limited to preventative measures and monitoring. Recovery from identity theft is a difficult, protracted, and messy process. Much of the current work views individual identity as a singular, natural element. An in depth analysis of personal identity reveals a person’s identity to be polymorphic and socially constructed. Capitalizing on the social view of identity exposes management techniques, like identity backups, to better enable personal identity recovery in the event of theft or disaster. Vignettes and examples illustrate principles for personal identity recovery management.

1. Introduction
Much of the privacy literature takes a monolithic view of identity. This view associates a physical person (hereafter a “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 his or her 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 protecting person’s privacy necessarily involves the ultimate production of their identity. That is,

\[ \text{privacy(person)} = \text{privacy(identity)} \]

In this conceptual paper, we suggest that there are new, additional privacy protection measures that arise when 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” [55, 6]. This terminology refers to an unwanted incident as a “bang”, and “left” refers to a timeline leading up to the incident (left leading to right). See Figure 1. The kind of management that is effective left-of-bang (predicated on prevention, prediction, probability, etc.) is rather different in nature than that which is effective right-of-bang (predicated on agility, improvisation, possibility, etc.). For privacy or identity compromises, right-of-bang remedial measures and recovery from loss are complex, ad hoc, and limited in effectiveness. Preventative measures have been 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 his or her identity and it is a first step to rethinking how we can better manage accidental or intentional privacy or identity 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.

The purpose of this conceptual research paper is to propose a novel model of individual management of multiple identities of layered types that support identity backup and recovery.

2. Socially Constructed Identities
Identity is important for understanding both individual and social human behaviors [29]. In the privacy discourse, the conceptualization of identity is associated with privacy loss or identity theft. The relationship implies recovery through privacy restoration or identity reconstruction. Yet the perception of privacy through the lens of identity is complicated by the
diversity of identity viewpoints. Identity authorities focus on differing aspects of the identity concept [44]. This diversity arises from the multifaceted nature of this concept [12]. For instance, identity explains many behavioral reactions in our lives whether these behaviors emerge from cultural, ethnic, or national differences [7, 33, 43]. It drives our life paths and decisions [27]. Identity also contributes to our sensible perception of strengths we draw from social and group affiliations [10, 42]. 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 [42, 2, 11, 53]. 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” [cited from 29, p. 1].

We draw upon Vignoles et al.’s [53, 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 [53, 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.

Authorities identify three levels through which identity are defined: individual, relational, and collective [46]. 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 [53, 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. [53]. Relational identity is also pertinent to how these roles are defined and perceived by the individuals who assume them [53]. In this context, many social scientists maintain that identity is defined and found within interpersonal space [3], families [31], or a larger structure [51]. Hence, an identity cannot be established by an individual on his or her own [53], in that it needs to be recognized by society [50]. 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. [53, p. 3]. Individuals can have material identities in that individuals view and treat material artifacts, such as houses, clothes, cars, contents of a bank account, as part of their identities [53].

In our analysis that follows, we compare and distinguish each of the layers of identity in terms of four elements indicated in the previous discussion: polymorphism, social constructivism, artificiality, and attributes. We describe each of these aspects first, and then describe each layer in terms of these aspects.

2.1. Polymorphism

Multiple identities exist within one individual or a group of individuals [53]. 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 [53]. However, they are not independent of each other but they interact with each other [1]. Moreover, “possible identities” is an area of study among social scientists that reveals the polymorphic nature of one’s identity. Possible identities are part of the future self. These are working philosophies attached to a potential, revised version of one’s future self, based on self-assessments of personal strengths, weaknesses, talents, and characteristics [37]. Possible identities have been studied within four main areas: life phases and transitions, socio-demographics, identity valence and balance, and identity distance [37]. Polymorphism is a focal characteristic of identity.

2.2. Social Constructivism

Identity is constructed from “the definitions and meanings of identity categories as ideas in their own right” [53, p. 4]. Identity categories, in any cultural milieu and historical time, have specific meanings that are socially established and constructed [53]. In addition, identity categories may be mooted, deconstructed [53], or even reconstructed. In light of such categories, identity can be viewed through ways of thinking/talking that appear to be salient in a specific social and historical context, yet independent of any one individual [40] because the categories are constructed through a concourse of social processes over history [13].

2.3. Artificial

Identities have different meanings in different times due to the historical and social construction influences. Moreover, identity is characterized by its pol-
ymorphic nature. These assumptions entail the artificiality of the identity establishment because one’s identity is devised differently depending on the cultural milieu, historical times [53], or one’s assessments of self-characteristics [36]. Hence, artificiality becomes another focal characteristic of identity.

2.4. Attributes
A discrete identity can be associated with certain kinds of attributes. Examples of such attributes include distinction, capability, and possession. Distinction refers to the clarity by which one identity can be distinguished from another. The most common example is the use of photographs on identity cards to clearly distinguish among individuals. Capability refers to the range of actions that accompanies an identity. A computer system login identity may be associated with a particular customer account, enabling that user to review past purchases. A different login identity may be associated with an administrator account, enabling that user to review other users’ past purchases. Possession refers to the attribution of ownership to an identity. For example, a bank login identity will usually attribute to that identity the ownership of money in associated bank accounts.

2.5. Onion Skin Model of Identity
Identity is not only a multifaceted social concept, its complexity becomes deeper when used in relation to advanced information and communication technologies (ICTs). This conceptualization problem is similar to that of culture itself, where social identity is too multi-faceted to measure. Straub, et al. [48] propose a virtual onion model in which the layering of the “virtual onion” is not a permanent and immutable set of relationships (p. 20). A collection of identities arises that can be represented as an onion skin model, especially when applying the concept of integrative identity [53] to the digital world. This onion skin model accounts for a nested set of individual identities, each enveloping and elaborating within it slightly more primitive identity concepts. For example, we will consider five identity skins or layers notable in the identity literature: physical identity, personal identity, social identity, online identity, and digital identity. See Figure 2. With the exception of physical identity, each layer may consist of multiple identities of the same type. We developed this collection of identities from the psycho-social research into fragmented identities, for the purpose of reconsidering certain fundamental aspects of privacy loss and identity theft in the digital world. This implies that the model is extensible such that future studies may expand it 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 and security.

2.5.1 Physical Identity. At the core of the model, the physical identity of an individual may be viewed as the information associated with the corporal body of that individual. While nonetheless a socially constructed concept, many identity management systems include the determination of whether an individual’s claimed identity matches their physical identity based on the physical hair, eye color, fingerprints, retina or iris patterns, facial geometry, height, weight, etc. [32].

With the mounting need of the verification of an individual’s identity, several factors 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 [23]. Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioral attributes of the person [24]. Compared to other systems, it is able to offer certain unique advantages such as negative recognition and non-repudiation [38]. In addition, biometrics cannot be easily stolen or shared, and it is also convenient to use without bringing the ID card or remembering passwords.

![Figure 2. Onion-skin model of socially constructed identities](image-url)
being increasingly used today to establish person recognition in a large number of civilian applications [25] 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 [17]. 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 [38]. 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 DNA information [14, 26, 57, 54].

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 and fingerprint, since 2006 [22]. It has improved the efficiency of border control and effectively advanced security controls over the illegal immigrants or terrorists [21].

India is the first large country in the world to implement a physical identity scheme at an unprecedented scale. The Unique Identification Authority of India (UIDAI) has chosen to use facial image, iris, and 10-print fingerprint rather than a physical ID card [41]. By 2014 half of India’s population will have registered in UIDAI [39], enabling the previously anonymous poor Indians to get access to services such as bank accounts, and driving licenses.

Physical identity, however, has certain limitations [35]. 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.

In terms of distinction, 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.

Regarding capability, the physical identity has important capabilities with physical possessions. Such possessions can be physically occupied or guarded and acquired or relinquished by physical transfer or trade.

With regard to the attribute of possession, the physical identity has the ability to possess tangible materials, e.g., gold, cash money, and household furnishings. In this case, the physical identity is physically associated with such material.

### 2.5.2. Personal Identity

Personal identity is “the individual self which is associated with close personal relationships and idiosyncratic attributes of the person” [29, 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? John Locke viewed personal identity as an aspect of consciousness rather than the body substance [52]. While extensively studied and debated, the notion of personal identity or the self remains contentious. The implicit meanings and philosophical perspectives could be one of the reasons this concept is murky. It is certainly distinctive; however, the distinguishing characteristics will vary from one philosopher to another. In our daily lives, we may perceive personal identity through a collection of attributes such as name, birthplace, or habits of dress. These attributes reflect the idiosyncratic attributes mentioned in Leary and Tangney’s [29] definition of personal identity. Capabilities associated with personal identity relate to these murky characteristics. For example, a person can change names, relocate and move house, or change citizenship. Possessions associated with this level of identity accumulate through being. Examples include personal knowledge and experience [19].

### 2.5.3. Social Identity

Social identity depends on an individual’s knowledge and sense of belonging with a group or community in a way that is of significant emotional value [29]. Social identity theory has been used to study group processes, collective self, group membership, and intergroup relations. Under the rubric of symbolic interactionism, a focus on the individual person regardless of the social structure, or vice versa, is partial and insufficient [9]. Citing Blumer [9] and Faris [20], Leary & Tangney [29, p. 2] define symbolic interactionism: “the meaning of things - including the self - is derived from social interaction, the reactions of significant others, and one’s interpretation of those interactions.” In this sense, social reality as well as social identity is so-
cially constructed. The social structural context plays a critical role in shaping identity [49]. Personal and social identities are deeply entangled: “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” [53, p. 5].

While the entanglement is inevitable, there are distinctions. The social identity is distinguished by its relation to groups and communities and the distinctive ways in which the individual interacts with others. The social identity entails a capability to connect and disconnect from such communities, along with acquiring, applying, or relinquishing symbolic or social capital. In a similar vein, the social identity can be associated with certain kinds of possessions, like social connections, roles in social networks, symbolic capital, and social capital.

2.5.4. Online Identity. Online identity is a social identity that is constructed through online interactions and communities but not offline ones [34]. The best examples are found among the social networks, communities and groups that operate across online social networking tools like LinkedIn, Facebook, Google+ and Twitter. They can be distinctive from other identities because an individual’s online identity can differ from their offline social identity (differing communities, groups, etc.). The capabilities of an online identity are also different, depending for example on the way the online software has been written or the online privileges acquired by a user through experience and expertise (e.g., a top-level restaurant reviewer for TripAdvisor). Such capabilities illustrate the new kinds of possessions that can accumulate to online identities, not only software-defined privileges, but also online symbolic and social capital (e.g., the number of Facebook friends).

2.5.5. Digital Identity. This identity is established as an individual inscribes his or her online identity onto various technologies. It differs from online identity in that the digital identity is mainly present in the way the individual has established their online identity using the available technologies. Digital identity is pertinent to the data that uniquely define a person and his or her relationship to other people [56]. 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 may be comprised of several attributes pertinent to him or her.

The digital identity is distinctive because it is more comprehensive than the online identity and can include other kinds of social relationships like business, financial, governmental, etc. It has the ability to possess materials, e.g., money in a bank account—an intangible but usable currency. The digital identity, which may be defined by a user name, password, digital token, etc., plays an important role in managing this account. The digital identity is actually capable of carrying out operations, e.g., managing a bank account, placing a purchase order on Amazon, contacting customer service, interacting with other people (and their other online identities) on Facebook, etc. As a consequence, digital identity capabilities often manipulate the online identity as a reflection of personal identity. One digital identity can be distinguished from other online identities by means of IP address, Gmail account, Twitter account, etc.

Some digital identity capabilities may be more subject to negotiation than those of online identity. An individual creates their online identity, but their digital identity is at least partly created for them. It is still a socially constructed identity. For example, bank account capabilities (such as automatic loans, overdrafts, or payments) must be negotiated with a banking institution.

Even though some attributes may correlate with the social structure, in this case, they belong to the individual him- or herself. Online identity is more related to social identity than personal identity, meaning that identity theft must be directly aimed at the digital identity but not the online identity, as it uniquely identifies the attributes required to seize a personal identity.

2.6. Changing Identities

Because these identities are socially constructed, we find multiple types of identity in the literature. This situation modifies our original monolithic view of identity to permit a one-to-many relationship between an individual person and their identities. (See Figure 2.) Identity becomes conditioned on which type of identity is under consideration (physical, online, digital, etc.):

\[
\text{person} = \text{identity(person, identity type)}
\]

The above reformulation states that a person is made up of different types of identity. This is a two dimensional socially constructed reformulation of identity. Our privacy formulation then becomes:

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

These varying, socially constructed types of identity may be connected in various specific ways. Let
us use the term actual identity to refer to the kind of singular identity set represented in Figure 2. Such would be the case when an individual person maintains a nested, consistent set of singular identities: there is only one physical, one personal, one social, one online, and one digital identity; and these are closely related to one another.

In some cases, however, individuals may choose to fabricate one or more identity that more-or-less contrasts their actual identity. Let us use the term fabricated identity for these contrasting identities.

For example, the distinction between online identity and digital identity is blurred in the literature. Online identity is a social identity that is constructed through online interactions and communities but not offline ones. Nabeth [34] defines online identity in a similar way yet uses the term interchangeably with digital identity. Charney [15], on the other hand, uses online identity to refer to what we describe as a digital identity.

Internet users communicate with each other for many 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 actual personal identity or actual social identity. This person could use pseudonyms and personal attributes that are an intentionally inaccurate reflection of his or her personal identity. Also, this person could fabricate his or her social identity in order to build a blended social identity that would better fit this aspirational online society. This person may fabricate an online identity using a new personal and social identity, deriving it either from his or her older personal and social identities, basing it on the new online milieu, or constructing it by synthesizing both previous and new identities. Such fabricated identities are already known to be frequent in online social relationships [5]. On the one hand, when a fabricated personal and social identity is constructed, privacy threats are less crucial because they do not form a threat to the original personal and social identity. This situation is an attractive alternative compared to individuals who use their actual personal and actual social identities in the digital world. On the other hand, when using actual or a blend of actual and fabricated identities, privacy threats grow more critical because they bring about a threat to the actual personal and actual social identity.

If the outer layer of our onion, the digital identity, is fabricated from a fabricated personal and fabricated social identity, digital identity privacy exposures have less effect on the individual’s actual identity. If the online identity is an accurate reflection of the individual’s actual personal and actual social identity, digital identity privacy exposures have greater effect on the individual’s actual identity.

3. Managing Identity

Two features of identity enable comprehensive individual management by a person of their own identity. Because identity is socially constructed, it can also be socially fabricated. It means an individual, along with the society in which they operate, can intentionally fabricate their identities. Society must adjust the legal system to allow this. Figure 3 represents a case in which an actual individual (Alice) possesses not only different types of identity, but different instances of the different types.

In this example, Alice’s actual identities are represented as the top part of our “onion”. Her actual physical, personal, social, online, and digital identities exist. Alice is also managing a number of fabricated identities. For example, she manages three fabricated digital identities that are based on her actual online identity. These three identities are named Bob, Carol, and Dan. She also manages a fifth identity, Erin, which entails a fabricated online identity based on her actual social identity, not her online identity.

3.1. Recovering with Backup Identities

The availability of intentionally fabricated identities enables the “right-of-bang” recovery that currently eludes privacy compromise events. For example, suppose Alice fabricates the digital identity Bob for the purposes of personal finance, and fabricates the digital identity Carol purely as a backup. With Bob she establishes the identity equivalent of a ‘last will and testament’ that leaves all of Bob’s possessions to Carol. If an identity thief compromises Bob, Alice can terminate this identity (i.e., Bob ‘dies’), and the possessions and capabilities of Bob transfer to Carol (an uncompromised identity). Since everything transpires between fabricated identities, the actual identi-
ty of Alice is insulated from the privacy compromise event.

### 3.2. Social construction properties of identity backup and multiple identities

Slicing the identity onion, as illustrated in Figure 3 requires social action, not just an individual action. In many developed societies, the notion of opening a bank account with a different name than last time is socially regarded as suspicious behavior. For a moment, suspend this suspicion and consider an alternative society.

In certain Native American societies, 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. Even outside such tribal societies, many people also go through similar, the not as deep, identity changes as they go to college, work, retire, move, marry or meet other life events. The tribal identity traditions provide a social 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 according to purpose and time. We might represent this evolution as

\[
\text{person} = \text{identity(person, identity type, purpose, time)}
\]

With the above representation, a person may acquire a collection of social, online, digital, etc. identities over their lifetime. The above reformulation states that, for our purposes in privacy, a person is made up of different types of identity, each of which may have different purposes and be different at different points in time. This is a four dimensional reformulation of identity. Our privacy formulation then becomes:

\[
\text{privacy(person)} = \text{privacy(\text{identity(person, identity type, purpose, time)})}
\]

The importance of social action in the fabrication of identities is critical. Commerce (e.g., banks), digital services (e.g., social networking sites), institutions (e.g., universities), etc. would choose not to penetrate through all identity layers and encumbering the physical identity.

### 3.3. Vignette: Identity recovery example

The following vignette illustrates how a polymorphic socially constructed identity sets up identity recovery.

Alice Peltoniemi, resides at 23B Sauna Street in Copperwood Michigan. Alice opens a bank account at the Copperwood Bank. Together Alice and the bank create an identity for Alice named Bob Brown. This identity, Bob 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) Alice’s. These attributes are Bob Brown’s, not Alice’s.

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

Let us suppose that the Copperwood Bank is hacked and totally compromised. Bob Brown’s identity, banking records, and credit card number are stolen. The identity hide enables a different form right-of-bang recovery. Alice and the bank create a new identity, Carol Green, different from both Bob and Alice, but with equivalent (not exactly the same) attributes. Effectively Bob Brown moves away from 23B Sauna Street in Copperwood Michigan, and Carol 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 Bob Brown’s privacy from cascading to Alice and Carol is a familiar issue of maintaining proper states in the identity system. An understanding of the onion model invokes well-known data confidentiality principles such as those in the Bell-Lapadula security model or the Biba integrity model [28].

Managing right-of-bang regards necessary primitive operations. 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 by authorized request from the 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 situations, 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 connected or disconnected with the physical identity of an individual. When the individual needs to incorporate a newly established identity, they use such a connection operation as associate. If there is a necessity to abandon an existing identity, it can also be executed by conducting disconnection operation as disassociate.

These primitive operations provide flexibility and agility in managing socially constructed identities and the physical identity. Such fundamental operations open ways to recover from incidents right-of-bang, adding more secure protection (recovery protection) to improve individual privacy.

### 3.4. Principles for 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 disposable privacy layer is feasible.

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.

#### 3.4.1. Legitimating polymorphic identities.

Current mores, laws, and regulations regard an individual 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.

#### 3.4.2 Protecting identity layers.

Current practices frequently span across identity layers, especially between the physical identity and the socially constructed identities. Limiting primitive operations to protect the boundaries between these layers is essential for avoiding compromises on either side of these boundaries from cascading across layers.

#### 3.4.3. Regulating polymorphic identities.

As well as regulating privacy, the state would 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, an enforcement package, including regulations, laws, framework, and standards, will be needed [4].

#### 3.4.4. 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.

#### 3.4.5. Implementing polymorphic identities.

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

### 4. Discussion and Conclusion

The monolithic view of a single, perpetual identity is becoming questionable due to the wide and grave concern over privacy protection. The onion skin model of identity contributes a novel perspective on identity management. Previous work has conceived of identity management in terms of government identity cards and systems [8, 47], organizational identity management [45], and interorganizational identity management [18]. The notion of identity backups often regards the data backup in an identity management system [30].

In modelling the identity compromise recovery problem in light of polymorphic, socially constructed identities, a more robust personal identity management system arises in which the individual controls their personal identity. This model however reverses the field of three factor identification. Currently one of the three factors involves physical identity. Our analysis reveals that this core identity needs to be the most highly protected from exposure. Recording fingerprints on easily misplaced or stolen laptops and smartphones entails an unnecessary and dangerous exposure. Employers, banks, and other organizations should be enjoined from collecting and holding such
data. Government agencies holding such physical identity data must govern it at the highest protection levels. (Alternative third factors are available, e.g., something you have, something you know, and something you do.)

A comparison of Figures 2 and 3 illustrates how personal identity management involves deconstructing the identity onion. This deconstruction amounts to slicing layers of the onion in such a way as to diversify the risk of identity compromise as well as provide recovery. Secured identities are truly polymorphic.

The management of socially constructed and polymorphic personal identities provides recovery in right-of-bang situations. It offers a solution for privacy compromises. It does not prevent them. It would prove most effective only in the context of the existing security measures to prevent identity compromises (such as caution in Internet use, avoiding Spam URLs, strong passwords, etc.). Likewise, existing personal identity protection, like insurance and monitoring are supplemented, not replaced, by recovery approaches like the above.

Future research is needed to explore the legal and legislative implications of polymorphic identities. Future work is also needed into the design of tools and software for managing polymorphic identities.

5. References


