Identity Hierarchy

by

Timothy Grayson

ABSTRACT:

Assuming a philosophical position on (social) identity, one can then consider how identity is created and perpetuated in the real world. Such an exploration revea ls an implicit hierarchy in the accepted practical structure of the existing system. Ignoring that hierarchy is sure to inhibit development of the digital identity system; a system that is likely to eclipse and encompass that which presently exists. Sadly, it appears that the digital identity development path is not building on the lessons of the past. It has the ambitious goal of creating an end-state of infinite digital identities while ignoring the opening-state of high-integrity "core" identity – for people. The absence of this foundational requirement will result in long-term system integrity problems. That will create opportunities for the creation, harvesting, and perpetuation of false virtual identities that could pollute the non-virtual world more rapidly and disastrously than ever. If we are concerned today with the creation of a robust solution to integrate the virtual world into our existing "physical" social world, it is incumbent upon us to not merely address the problem within the boundaries of existing structures and requirements, but to use the capabilities of developing technologies to increase the integrity of the system for all purposes in all places.

Identity Hierarchy

by

Timothy Grayson

I. Building on a philosophy of identity

In an essay entitled, *Philosophy of Identity,* I outlined a practical philosophy of social identity: what social identity is. In this paper we go further to consider how identity is created and perpetuated in the real world. A key discovery is the implicit hierarchy created by the accepted practical structure of the existing identity system. To ignore its existence and lessons – let alone its necessity – is to imperil the development of the nascent digital identity system, a system with the potential to eclipse existing methods and structures. Unfortunately, the development path of *digital* identity has not followed that of identity in the pre-virtual world. Some would attempt to create an end-state of infinite digital identities by denying or avoiding the essential creation of an opening-state "core" identity. The absence of this foundational requirement will result in long-term system integrity problems.

In this paper we build on the notions of identity as a social construct given meaning by attesting credentials as set forth in *Philosophy of Identity*. Some startling incongruities become evident through the exploration of the physical and virtual identity experience to date. Moreover, the importance of various credentials, the value in the hierarchy, and the potential for problems resulting from the virtuality of a physically-bound identity will be revealed. Within this context, we examine the specific nature of *core identity* and persona as requirements of identity in the broadest sense, both online and off. All of which is made possible by judicious use of credential "artifacts" to evidence the identity.

II. Identity's hierarchy

We do not internalize identity, which is to say that our identity serves no internal purpose.[1] Alone on a desert island, our identity beyond being human is moot. Only in the social context is there cause for identity, which makes identity internalization a process of relativizing (i.e., of comprehending ourselves *as* somebody *relative* to others). In the social context we project identity in person, via images, and through words. Implicit in this projection and social acceptance of identity is the identity's *a priori* existence in some understood form. In this sense it is therefore a notional definition of what, or who, a person (i.e., a single living human entity) is within the broad social environment. Moreover, the identity is presumed to be singular. That is, we expect

[1] Not, of course, the internal purpose served in its generation by/for the "self." This discussion is more practical and social. We'll try to avoid any kind of psychological assessments.

one identity to map to one individual. Identities are not shared by several people nor should one individual be known by a multitude of identities.[2]

Given the relatively limited likelihood but potentially harmful impact of false identification, receivers of an identity assertion typically seek corroborative evidence of an its validity. As projectors of identity, we augment and support our assertions with official or otherwise audience-acceptable documentation. Particularly in non-trivial commercial or other "official" activities, and especially activities conducted at a distance, identity is highly dependent upon such external proofs. These proofs are often referred to as credentials, and, although that is exactly what they are, the meaning of the word "credential" may be confusing. To make the distinction certain, we'll refer to these manifestations of identity – these proofs supporting the 1:1 mapping of an identity to an individual – as identity *artifacts*. They are, after all, what is left behind to support the claim that there is or was a unique individual at some time.

In the physical world, identity artifacts are well understood. Certificates attesting to birth, name change, marriage, death; licenses to drive, travel, obtain medical care, and so forth; access authorizations for physical installations, credit, affiliation privileges, etc. *ad naseum* are commonplace artifacts. Today, artifacts may be physical or virtual, although we generally tend toward those we can see (even if only for visual comfort). Consider, for example, a national citizenship number such as social security or social insurance. Although issued with a plastic card, it is the number itself that is broadly used – virtually not physically. Oftentimes, such as with the social number or driver's license, our familiarity with and confidence in an artifact leads us to use it for many purposes besides the one(s) for which it was designed.

One of the features of the identity artifact system that exists all around us is the implied and necessary hierarchy among artifacts. Moreover, within that hierarchy the process and flow for (legitimate) creation of identity artifacts is well established. Quite simply: some artifacts are stronger and more reliable than others; stronger artifacts beget weaker, and never the reverse.

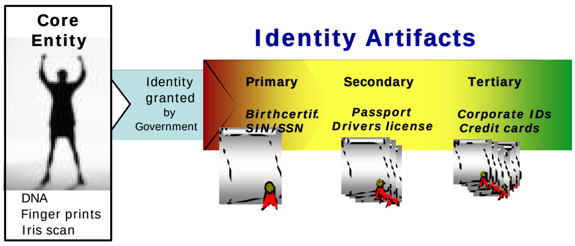

Figure 1 – Fundamental identity hierarchy

Figure 1, above, shows the arrow of development for a 1:1 mapping of a unique individual to an identity as conveyed by artificial evidence. From left to right, the entity or individual is granted status as a unique individual by the acknowledged formal authority – typically a state. A state initiates this process – upon request – by issuing certain *primary* artifacts upon satisfactory evidence that the artifact is required. Foremost amongst the state's primary artifacts is the birth certificate and, more often than not, a social membership (e.g., social insurance or social security number).[3] Primary artifacts typically attest to immutable identity characteristics. Some, however, such as the social number are not attestations to characteristics as much as they are attestations to an individual's authenticity *in toto* by way of state recognition of that individual. Regardless, primary artifacts have

[2] For the arguments to support these assertions see *Philosophy of Identity*.

[3] Even at that, the social membership is often generated years post-fact, creating systemic problems. Of course, this is an unintended consequence of this social identity document being used for purposes beyond which it was created or intended.

a singular, direct, 1:1 connection with the individual. The primary artifacts effectively "create" the social identity, or its foundation at the very least.

The individual strengthens and broadens his/her social identity by using primary artifacts as "breeder" documents to generate additional artifacts. The fullness of an individual's identity – roles, freedoms, memberships, associations, etc. – depends on proofs that exist in the many other artifacts beyond the primary attestations to existence. These other documents are temporary and, while their connection may be distant, are typically tied to a primary artifact in some way.[4] The temporariness of these other artifacts that we rely on most best documents and addresses evolutions in an individual's social character and broad identity. Thus the system has both flexibility and integrity.

One type of derived artifact is the *secondary* "official document" such as driver's license, military identity, and passport. These secondary artifacts are typically created for a singular purpose, as the examples would suggest. They are equally typically used, however, for purposes well beyond their original intent. Because they are "official" documents, these artifacts are often accepted as valid and reasonable substitutes for other secondary artifacts. An excellent example is how the driver's license is used as proof of identity for domestic air travel and age of majority. Secondary artifacts often attest to the individual's immutable identity characteristics (e.g., eye color, etc.), so they become a *de facto* primary artifact for wide usage in the broadest context. As a result of their official issuance and *de facto* substitution for primary documents, secondary artifacts are themselves often the breeder documents for *tertiary* artifacts.

The most prevalent but least-well uniquely mapped to the individual could be called *tertiary* artifacts because they are at least one generation removed from the identity-creating artifacts.[5] Tertiary artifacts might include corporate affiliations, credit cards, bank account numbers, library memberships, and so forth down the line through to diplomas, professional certificates, frequent flyer accounts, and even video rental memberships. Their identity value beyond the declared purpose is limited. Generally they are unofficial and have limited – although potentially valuable – utility. But, tertiary artifacts also fill out the identity as a result of the information and/or understanding about the individual that could be inferred from the artifact's mere existence, never mind the stockpile of associated data. Tertiary artifacts fill out the identity by adding the texture of persona to the framework of core identity.

Obviously, artifact integrity is highest near the core and deteriorates with distance. There can be no doubt that a (genuine) birth certificate is of greater import and credibility viz. the individual's *bona fides* than a driver's license, which is yet greater than a fitness membership card. The reason, of course, is because of the permanence of the primary artifact. But extensive use and over-reliance on primary artifacts is cumbersome and risky. The alternative to such a rigid and cumbersome mapping is the more transient tertiary artifact; the perfect complement that gives the system resilience and flexibility. Primary artifacts are *deep*: they are unchanging and desired to be private (or at least opaque). Tertiary artifacts are *wide*: they change and can be changed; the features and information they represent are typically superficial, incomplete, readily accessible, and – often – transparent.

[4] The only exception is the creation of "false" documents.

[5] Some tertiary artifacts are derived directly from the primary artifact(s). Their status is nevertheless reduced because their direct 1:1 connection to the individual is more tenuous and their use is extremely specific.

The greatest risk of impersonation and misrepresentation is at the further edges of the tertiary space. This is particularly true where for cost:benefit reasons the issuer opts not to derive its artifact from another of higher quality.[6] The logical and practical effect of such a creation process is an unreliable artifact. For a number of reasons, not least of which is weaker measures to assure the authenticity of both the artifact and its representations, tertiary artifacts are more readily misused. Note that where a tertiary artifact is not derived from a stronger credential, even in-person proofing, which emulates stronger 1:1 mapping, does not lower the risk. To effectively strengthen the identity artifact creation process, IPP must correlate with core identity as provided in the primary or secondary artifact evidence. Regardless, tertiary artifacts are the most insecure and least *systemically* valuable viz. authentic identity.

III. Digital identity: evolution not revolution

Keeping with the real world tenet that stronger begets weaker, we do not build (or perhaps *ought* not to build) identities from right to left in the model (Figure 1). To preserve the integrity of the unique, individual mapping system that has evolved and stabilized in the developed world over the course of centuries, legal and socially valuable identities for individuals are not created based on frequent-flyer or debit card or enterprise employee artifacts. Most certainly, any such "identity," represented primarily by a tertiary artifact, would have no official status or purpose beyond the intended bilateral use between issuer and holder. Yet that is exactly what some recommend be done in the virtual world. Figure 2, below, depicts a second flow more closely resembling current concepts for/development of identity on the Web – at least in North America. Notice how the tertiary digital artifact creation originates digital identity and *presumes* then *implies* the existence of a legal, tangible identity without creating a 1:1 map connection between the physical world and the virtual world at the appropriate (i.e., strong) place.[7]

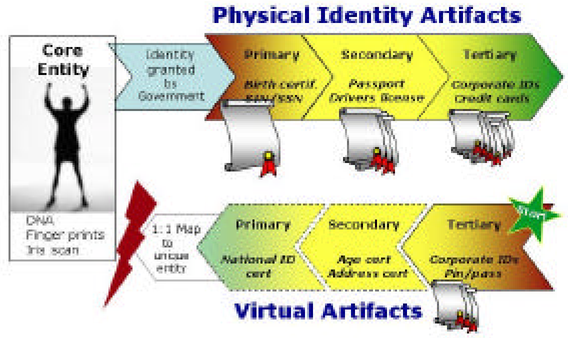

Figure 2 – Attempting to reverse the hierarchy

For all intents and purposes, in this model the artifact-based identity systems of the physical and virtual world remain detached and operate in parallel. Even if the link is made so that the tertiary *digital* artifact is derived from a primary or secondary physical artifact, it ought to have no greater strength or effect than a tertiary physical artifact. In other words, the link between physical and virtual systems has to be made so that primary (or secondary) digital artifacts are derived from their equivalent in the physical system and that no digital artifact of greater strength can be derived from one of "weaker" strength. The current course of federated "existing-relationship"-based identity would leave the digital environment without essential 1:1

[6] Tertiary artifact issuers with a high commercial reliance on their artifact, and who bear liability for its proper issue and life-cycle management (e.g., credit card issuers) address this problem with measures such as (a) deriving the artifact from others of higher grade/quality, (b) relying on alternate reports on and histories of the individual/identity (e.g., credit reporting), (c) placing exposure limits that match the level of certainty they have in the identity (i.e., low credit with subsequent increases based on history), and (d) implementing some form of in-person proofing.

[7] The creation of the secondary and primary digital artifacts presented in Figure 2 is notional. That is, it depicts the effect of present proposal/activity, although no new "real" and "official" secondary or primary artifacts are being created.

systemic integrity and no way to create or evolve to such a state.

Which is all to say that, among other things, digital identities are being propagated by derivation at the weakest point in the accepted identity system: at the furthest distance from the core entity and most deeply reliable primary artifacts. There is no argument that such a state is not inherently weak. The argument that these digital identities are being created for limited purposes or are permitting one to take advantage of identity relationships that already exist for other purposes does nothing to refute the conclusion. It does, however, go a long way to support the contention that pre-existing relationship-based identities have limited *systemic* integrity and value. Such a system of distributed digital identity *creation* based on a multitude of pre-existing (commercial) relationships then becomes an identity time bomb: falsely robust and lacking resilience.

In the world we know, it is generally not possible to induce a valid core identity (i.e., alter primary characteristics and artifacts) using weaker evidence (i.e., identity documents) – even a preponderance of such evidence. Credibility flows down, or to the right in Figures 1/2. For instance, a driver's license will likely not be reissued on the basis of three credit cards, a facility access from work, and NRA membership certificate. All these tertiary artifacts do not equal a secondary artifact. More likely, complementary superior artifacts (or notarized attestations) will be required. Why then, should the system of digital identity attempt to do precisely that which is established *worst* practice?

Some would argue that many shallow digital identities can co-exist with one or more deeper, more systemically valuable (1:1 mapped) artifacts, and that the issuer of the said artifact/credential would take responsibility for the identity they've created. Co-existence of many digital identities in the form of a multitude of unique artifacts will undoubtedly persist just as today in the physical world. That, however, is not the issue. The more significant issue is that the artifacts in the real world *and* the virtual world are generally, in fact, tied together in a one-way chain of reliance or derivation. And, the root is necessarily stronger – or deeper. So, for another reason, the primary artifact *must* come first.

Responsibility for the attestation by the identity issuer raises two significant factors: acceptance of liability and temporality. How long and how far will an employer stand behind an employee's identity, a bank behind its customers, where the person/identity being guaranteed is using the identity and potentially creating liabilities for the issuer in contexts unrelated to the relationship (e.g., the employee digital identity being used for non-work purposes)? That unauthorized, maybe misappropriated attestation of identity may be the necessary and sufficient condition to derive other, possibly non-trivial activities and identities. If the reliance is explicit, legal liability may and moral liability will surely persist.

Quite likely there will be residual life in the downstream transaction – a warranty or guarantee of some sort – directly or as a part of an explicit reliance chain within "circles of trust." Given the very high likelihood of a discontinuance of relations between the parties (issuer and "identity") to the pre-existing relationship upon which the identity attestations were based, and the endurance of legal and moral responsibility, how does the "pre-existing relationship-based, circle-of-trust, and no primary artifact" system hold up? Although a bank may stop attesting to and allowing others to rely on their customer's identity when the commercial relationship ends, earlier attestations and downstream results persist. Downstream results could include derived identities created on the basis of the bank's original attestation, liabilities for actions, and so forth. These results that continue may create liability to the original bank because of the reliance placed on them (and if there is no assurance in the reliability of the credential, its value is exceedingly limited). What if the bank's original identification/authentication of its customer was defrauded or mistaken to begin with?

Consider a horrible example: An individual opens a simple relationship (e.g., personal chequing account) with a bank on the basis of fraudulent information. The bank creates a digital identity (not a mere artifact, but a bank-specific identity with artifact attached), which others in its federated circle of trust willingly accept. Based on this wide acceptance of the identity and the rather ordinary transaction history that develops, others issue separate identities. A credit card gets issued. Iterations continue and eventually those evidentiary items are used to gain the necessary access for an act of terrorism. Meanwhile the core entity's *true physical identity* is hidden as a result of there being no systemic link back to primary artifacts of core identity and a 1:1 map between (virtual) identity and physical entity. So much for peaceful, unmediated co-existence of a multitude of "identities."

I concede that in the extremely limited context of identity programs with the limited (i.e., single-use, person as corporate agent) concerns of the enterprise environment in mind that the challenge of 1:1 mapping could be unnecessary. After all, in this particular "role" the enterprise is taking on the liability of attestation to identity and making assurances of authenticity for its commercial purposes. The individual is merely acting as an agent on behalf of the enterprise. So long as the enterprise controls the artifact and its use, both authorized and unauthorized, there may be no problem. It does, however, raise the issue of whether the so-called identity is that of an individual, with all the rights attached thereto, or of a virtual entity sharing a name and certain characteristics with some individual. It also raises a question about the proposal's long-term karmic integrity. (i.e., Does this expedient, narrowly-focused implementation possibly embed itself, quite unintentionally, as a long-term encumbrance on the system?)

Two issues render suspect the organization and its ability to maintain the integrity of the virtual system as it migrates to the open environment beyond the organization's direct control. First is the matter of the individual as agent. In practice, few individuals are mere agents of the corporate body. And, given the high likelihood of slippage (i.e., an individual's misuse of the artifact and the complicit acceptance by (unauthorized) relying parties, such as a corporate charge card being used for personal expenses), the willful avoidance of a 1:1 map for each individual issued any digital credential – artifact – creates a gap for breach of system integrity. Second is the issue of how artifacts are used to breed other artifacts. Identity is, of course, the sum of the artifacts that support it; not any single artifact. Because there is no established system or means for how such derivations may be done, the first artifacts have a tremendous propensity to be used as breeder documents for wide-ranging and robust, but "rogue" identities. Who is to say that with unmapped artifacts (i.e., untied to a unique physical individual) being created for limited commercial purposes such as that described above, other digital artifacts won't be created to perpetuate and substantiate ultimately false identities? Worse yet, what if those suspect virtual artifacts are used to generate traditional physical identity artifacts in the real world – as described in the earlier example.

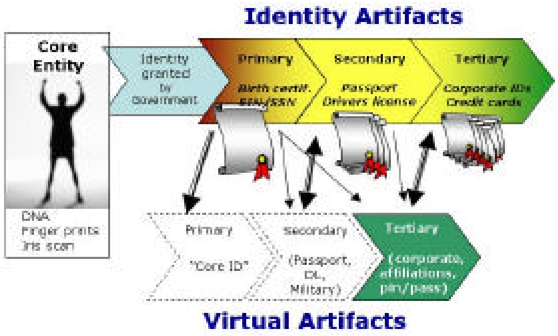

Figure 3 – Properly bridging physical and virtual

While it may be expedient for any single-use "identity" (artifact) provider to examine requirements of its digital identity needs in isolation, doing so in the globally networked environment raises the risk of loosing a genie from the bottle. Any such action is nothing if not short-sighted. The emphasis by technology solution providers on processes that contemplate the issuance of multiple identities to any single individual while avoiding the messy issue of 1:1 mapping between the physical and virtual worlds is patently wrong and misguided. The system breaks down under stress and extensive use, i.e., the kind of general, multi-purpose use of digital identity that we see as holding greater value than the one-to-one identity relationships (i.e., single-use enterprise "identities") that can exist today.

The process is flawed and creates massive openings for misuse, fraud, and irreparable degradation of both the emerging (virtual) and existing (physical) systems. As envisaged by its predominantly technologist propagators, digital identity is effectively detached and isolated from the physical world system, which presents the problem of duality and persistent inter-system integrity problems. Ultimately, the two systems are at cross-purposes like competing standards (e.g., VHS v. Beta). The lack of overall system integrity creates opportunities for the creation, harvesting, and perpetuation of false virtual identities. If, as I presume, we are concerned today with the creation of a robust solution to integrate the virtual world into our existing "physical" social world – commercial or otherwise – it is incumbent upon us to not merely address the problem within the boundaries of existing structures and requirements, but in fact to use developing technologies and the capabilities they afford to increase the integrity of the system for all purposes in all places. Let's look to the past and present for a glimpse of the future.

XXX

Timothy Grayson is part of the eBusiness group at Canada Post Corporation. grayson@templar.ca