Portable Identity

OVERVIEW

Portable Identity is the right and responsibility of each of us to create, control, and carry the important pieces of information that define who we are in a private, secure, and trusted manner. Other individuals, entities or authorities may validate (or “attest to”) various aspects of our identity, but portability implies that we ourselves own and manage our identity details and determine what others know about us in any given context. The reciprocal right of others to know enough about us to feel safe to interact with us effectively creates a “need to know” standard for sharing information about our identity. The “need to know” standard defines what someone reasonably requires to give us permission to act in a situation that requires some level of authorization. That standard might require very different things in different instances – for example, receiving a payment from someone might require much less information than extending credit to that same person. The extent to which a person is able to operate freely in a world of portable identity will correspond to the trust that person can establish through their identity details and associated attestations.

The tension with portable identity is balancing the privacy rights of the individual with the security needs of society, in a manner that maximizes trust that permissions to act are valid. When trust is present, portable identity acts as a catalyst that engenders minimal friction, appropriate privacy, and maximum inclusion – all without incidentally serving as an accelerant for exploitation by those who would use portable identity for abusive ends.

In a world where not everyone agrees or gets along, the very definition of “bad” to some is likely a “good” attestation to others. For this reason, portable identity is most effective when participation in the identity framework includes those that some would call “bad actors,” because inclusivity brings the shadowy parallel world of black markets under the disinfecting transparency of sunlight. A high-level framework that includes everyone does not require those who do not wish to deal with each other to interact; on the contrary, such a framework enables more accurate identification of true bad actors or those who for various reasons do not wish to deal with each other. Regardless of subjective labels, the need for privacy, security and trust is a matter of methods that can operate in a neutral manner across the entire population (including individuals, entities, and the assets/permissions controlled by those parties). Just as standards such as SMTP and SMS allow email and phone networks to operate on our behalves, even between parties in conflict, so too can portable identity standards appropriately enable/restrict our permissions to act, even in situations where there are disputed views over the appropriate authorizations and permissions for a particular identity.

PORTABLE IDENTITY AS A STANDARD

The notion of portable identity operating as a standard rather than a proprietary method implies that any single company, industry, or country approach to identity is inappropriately siloed by its very design and nature. Portable identity, by definition effectively operates as a standard that works *across* companies, industries, and countries. What portable identity does not, and cannot do, is determine specific permissions associated with each country jurisdiction, industry rule set, or company policy and procedures. For example, while Tanzania and Switzerland may have compelling reasons to define differently the types of identifying details required to establish a person's identity, the underlying framework of how identity details are stored and shared can be the same, making it possible for a person to operate in both countries with a single, portable identity validated under two different identity systems. *Thus, the power of policy makers, regulators, and law enforcement is not diminished by portable identity – it is just differently enabled*.

PORTABLE IDENTITY DEFINITION OF TERMS

Portable means something we take with us without having ever having to leave behind or re-establish. **Identity** is something we know to be what we think it is, rather than potentially confused or mistaken as something else.

THE ROLE OF UNIQUE NAMES FOR PORTABLE IDENTITY

The most compelling example of something we humans have created that personifies portable identity is a name (and in particular a unique name). While some names like John Doe are only semi-unique, human language affords us the combinatoric possibilities that enable every one of us (and every entity, and even everything) to have distinct and unique names with no overlaps. Email addresses already meet this norm (when combined with an @ domain suffix such as username@gmail.com). And so do phone numbers (when combined with a country code such as +1 for the United States). Without that uniqueness, neither the SMTP or SMS standards would work as definitive routing standards for moving data from one endpoint to another.

The existence of domain suffixes and country codes is a concession to naming conventions that are globally enabled as unique, but not fully portable for the user. One cannot take one's Google email address and have it hosted by Yahoo. Conversely, one can port one's phone number between phone companies in the U.S., but not between phone companies in different countries.

In our vision for a truly portable identity world, one's named identity truly belongs to each of us, rather than rather than to any government or company. In such a world, we should be able to have multiple identities – perhaps one more personal and private versus one that is more public and role-based – but there would be confusion if the names associated with those identities were not unique in themselves. Like Twitter and Skype handles, you wouldn't want to be mistaken in understanding who you were listening or talking to. Nor would you expect to lose or switch a name simply because you moved overseas, changed your phone, switched jobs, or changed where you banked for that matter.

Keeping your name would be a right and a responsibility – especially if you built up a reputation with that name. Granted, names might be passed on when we die, transferred for business purposes (in the case of a branded entity like Coca-Cola), or created or released for other specific purposes. While associated with a set of portable identity details, names themselves should operate as persistent identity markers, with any changes reflected in a permanent registry.

SECURING THE NAMESPACE THROUGH THE NEUTRALITY OF BLOCKCHAIN

The list of all names, known as a "namespace," would be a public good in the context of establishing a portable identity framework. The list must be public and viewable by all, or else there is no way to determine that the attempt to create a new name is not a duplicate of one that already exists. The existence of blockchain technology suggests that such a list can operate without a central authority so that even parties that might disagree on many other matters can at least agree to not create duplicate names. Internet addresses (i.e. the unique numbers behind each unique web address) are another example of a namespace – albeit one that was created prior to the existence of distributed ledgers –

that allow assurance of uniqueness without a central authority. In the case of portable identity, there is the opportunity for a fresh start with a neutral blockchain architecture to support ownership and portability of identities even where various companies, industries, and countries (along with their regulators) might not be able to otherwise agree and cooperate.

ATTESTATIONS ABOUT OUR NAMED IDENTITIES

A namespace without attestations about the identities of the holders of the names is hollow because nothing can be trusted about the names in question. The reason Twitter has "verified" accounts is so that one can tell the difference between a satirical account named "@DonaldTrump" (with only 5,000 followers) and the "@realDonaldTrump" (with over 24 million followers at the time of this writing).

A name is only as good as its attestations – which can be determined by the sheer number of followers in the Donald Trump case above, *or* based on the quality of the attestation agent (i.e. Twitter as a corporation doing its own due diligence and endorsement of which accounts can be verified). Note that Twitter's attestation that @realDonaldTrump *is* truly Donald Trump is an objective attestation in contrast to a subjective rating (which might indicate something about the goodness/badness of the party behind name). Though we increasingly live in a fact challenged world, the notion of attestations returns to (and relies upon) a distinction between attestations (which is *notation* of a particular statement *at a point in time* about someone or something *regardless* of whether it is true or false) versus ratings (which are *inherently value based* expressions of relative desirability regarding one or a combination of attestations). In essence, a workable namespace must divide the question of "is this person this person attested to about a specific fact or status, or not." about their identity, versus "is this a good/bad person." A true namespace humbly is the focus of the former, while credit bureaus are left to ponder the later.

Attestations about an identity can come from a variety of traditional sources (employers, government agencies, utilities, universities, etc.) or emerging but less traditional sources (social media, biometrics, people in one's contact list, etc.). Attestations may include both a testament that someone is who they say they are, but also that they have achieved certain levels of credentials that increase confidence (and ratings) about their capabilities/standing rather than just the correctness of their identity.

THE PUBLIC LEDGER OF ATTESTATIONS

When attestations are written to a public ledger – especially one that is confirmed as full, validated and immutable by blockchain technology, then *one's attested identity becomes portable because it is transparent and equally available to all*, rather than trapped in a view accessible by only one company or country. The notion of portability is based less on the fact that the party concerned physically carries their personally identifiable information (PII) around (though they do so on a mobile phone), but rather than the attestations about that data sit on and are universally viewable on a public ledger.

Publicly available attestations can and should be designed to preserve personal privacy. Note that an attestation is distinct from the underlying information that is attested to – which may be encrypted and not visible to public view. An example of an attestation verification from a third party might be that I can log into a bank account and that the address details therein *match* those that are on my government ID and phone account. No mention is made of which bank my name is associated with, or what any of the address details were that matched up between my bank, government ID and phone account.

The discoverability of all attestations creates a public good that allows a person to control and carry reputational capital associated with their name. The reciprocal balancing of privacy rights and responsibilities implies that an individual has a right to choose which attestations will appear in a public register, which they could do by co-signing the attestation with the attestation agent. Once the decision is made to approve and sign an attestation, that attestation is openly and equally accessible to all. Without full transparency on an open and equal basis, partial/uneven access to attestation information could result in asymmetrical knowledge about identity for some parties versus others. Equal access to identity markers is meant to be a baseline for society and a fundamental right for individuals rather than a source of selective and biased advantage relative to another's more limited or constrained access.

TOKENIZATION OF PORTABLE IDENTITIES

For much of the past century, most people encountered portable identity through an ID card and/or passport. The ID card/passport stated what your identity was and could easily be carried with you, and thus served as a portable token of your identity with third parties who wanted assurance of who they were dealing with. ID cards/passports have historically been issued "top-down" by authorities (companies and countries) to holders. Attestations about the individuals have been stored in siloed databases that can be checked with increasing (too much) ease through the web and mobile devices. Lost, stolen, and counterfeited ID cards are a staple of crime and spy intrigue. Hacking the silos of data behind the ID cards has moved from a sport to a full-on black market industry preying on the duplicative explosion of siloed but poorly protected PII under today's status quo business/risk/compliance practices.

The last decade has seen development of transformative technologies that offer the possibility of taking portable identity to another level. The ubiquitous availability of mobile phones, GPS, encryption and the emerging availability of biometrics can be brought together to create a modern, digitized form of ID card, and with it possibilities for more effectively tokenizing one's identity.

While cards and passports have gotten smarter with the advent of embedded chip technology, the capabilities of the mobile phone have gone much further and faster. It is now possible to imagine that every person above a very young age will have access to a powerful mobile device that can be connected to the Internet and thus the afore-mentioned public namespace and attestation databases supporting portable identity. But more than attaching to those databases, the mobile phone can serve as the starting platform from which individuals create, control, and carry their tokenized identity – all core tenants of the rights and responsibilities of portable identity.

ID cards (especially payment cards) may still have their place as a convenient tokenized form of ID, but the advent of mobile phones suggests that cards will act more as companions to a fully featured portable computing platform that gives users much more capability than can ever be operated through a relatively passive form factor like a mere card. While a card can still be used as a token for authorization, the mobile phone can be used to i) actually select/create a new namespace entry; ii) self-attest that the newly created name can be associated with a particular phone number/SIM card/physical phone; iii) cross reference though the contact list of the phone persons that appear in each other's contact list that also have a portable identity; iv) track and construct a location map where permissioned activity normally does and does not happen for a particular identity; and v) collect and privately/locally store in an encrypted form personally identifiable information that can selectively be attested to on a "need to know" basis for inclusion in the public attestation database. Furthermore, the mobile phone itself, when safeguarded with access via biometrics or a PIN number, can reduce or eliminate the need for the inherently insecure reliance on username/password controls for access to key permissions.[i]

REVOKING AND RESTORING PORTABLE IDENTITY

Because portable identity is truly created, controlled, and carried by individuals, there is no need for a central authority to take a controlling role when the need arises to either revoke or restore identity. When the token that controls identity (i.e., the mobile phone) is lost, stolen, or otherwise compromised, how then is the identity associated with that token revoked and restored without a reliance on central authority?

The answer lies in a key but limited set of governance rules. Under the governance rules as we envision them, as part of creating each portable identity, the identity holder nominates individuals from their own trusted contacts who can serve, when necessary, in a power-of-attorney capacity to revoke a lost/stolen/compromised identity temporarily until the rightful owner can establish themselves on another mobile device. Each identity holder designates third parties who they trust to act on their behalf to revoke or restore their identity if a situation so demands. A smart contract (such as a rule that two out of three nominees can act to revoke) allows immediate termination of all permissions associated with a compromised name, and control of the actual name switched off on the mobile phone of the compromised party.[ii]

There is nothing to stop an individual from nominating an entity (i.e. their lawyer or accounting firm) to act as their power of attorney – but there is no reason that the chain of command cannot simply rely upon a family member or web of trusted friends. The point is that there need not be reliance on a central authority to establish a clear line of control over the permissions associated with any portable identity.

Certain countries may choose to require as a matter of law that designated authorities have the power to revoke control of a name via their own norms of due process. Similarly, certain countries may also dictate that their governments have access to certain personal information that an individual has entered on their own behalf. The converse is also true – that certain personal information may legally be non-sharable without the explicit consent of the individual who controls a name. Such decisions could be made in accordance with local norms and political systems - nothing in the architecture of portable identity implies any minimum or maximum legal limits that regulators and law enforcement in a particular jurisdiction must or must not enforce as a matter of law regarding rules for creating, controlling and carrying identity. But such rules are a layer of controls overlaid on the fundamental enablement of portable identity – which is agnostic to any specific set of rules regarding the trade-off between privacy and security that plays out in each nation state around the world.

IMPLICATIONS OF A WORLD WITH PORTABLE IDENTITY

First and foremost is the notion that everyone (and every entity and potentially every "thing") has a unique and identifying name or names. This is an inherently inclusive world as a starting construct, whatever challenges may be associated with moving away from today's status quo of incomplete, static, and siloed identities. Directionally, portable identity is a path to complete *inclusion of all persons wishing to be trusted enough to interact with one another -- without the reliance on a centralized and dominant company or country to act as Big Brother to enforce participation and compliance*.

In a world of portable identity, every individual starts with an inherent ability to do (technologically) certain things if their mobile phone works (i.e. can validate a mobile phone number and connect to the internet). Even with nothing more than a (free) virtual mobile number to serve as a first attestation to a unique name, the minimum requirement for a portable identity is met. That name holder can then be "found" as an endpoint that can be communicated and interacted with. In much the same way that SWIFT operates as a network of endpoints for one financial institution to find another and send messages about moving value around, portable identity extends the paradigm to a network of endpoints that potentially includes every individual, entity, and thing in the world *and the dependencies/ownerships between those markers*.

Whereas SWIFT operates as an authoritative operator of its network that includes and excludes actions based on its own rule set, portable identity is inherently open about its membership and potential scope of applicability to permitted actions. However, portable identity's openness does not imply a lack of controls over authorization and permissions. On the contrary, actions between parties who choose to interact are completely "at will" under portable identity -- based on the publicly observable level of attestations that provide the foundation to authorize, limit or deny execution of a particular permission at a particular point in time by the parties to that activity.

An illustration of the extent and limits of the power of portable identity can be seen with the specific use case of holding/sending/receiving/converting and spending value – a core permission in our exchange-based society. A mobile/internet enabled portable identity attached to a distributed ledger like Bitcoin suggests that any name can be associated with public key/private key pair that allows value to be sent/received/held without reliance on third party custodian. While Bitcoin can be traded today without intervention of a central authority, lack of a supporting, comprehensive identity system means that such transactions often take place without the benefit of operational and legal assurances, limiting the appeal of such trade. The binding of a name <-> phone number <-> public key suggests that, as a practical manner, anyone with access to the internet can send/receive/hold value with the assurance that they know who they are dealing with, but without the need for further consent or control of a company or government. Converting that value into another form of fiat, or spending it through traditional bank or card networks does require interaction and consent of traditional company and government regulated networks. But significantly, much freedom of action is enabled independently of any central authority, substantially lowering or eliminating the bar to financial inclusion for everyone in the world.

SHORTFALLS AND PITFALLS OF CURRENT BSA/AML/KYC/CIP/OFAC REGIMES

Current BSA/AML/KYC/OFAC rule regimes were not designed with portability of identity in mind and should be enhanced to reflect the fact that central operators will no longer control access to large swaths of permissioned activity that can be undertaken when identity is truly portable. Managing top-down in a world that is enabled bottom up is unlikely to safeguard privacy or security, let alone engender trust by citizens.   *A more realistic regime for BSA/AML/KYC/OFAC would vest more responsibility for monitoring by specialized/interested/authorized parties looking at activity by individuals/entities across companies/countries rather than myopically within silos (which is easily defeated/exploited).*   At some point, the notion of siloed policing by private parties may be able to give way to a more holistic approach to security (while still respecting privacy); such an approach could make new inroads into criminal and terrorist funding capabilities. Construction of, and access to, a public namespace is a foundational shift that could enable a transformation of the current regime of highly manual OFAC checks and SAR filings to a powerful, automated and portable KYC regime that has global reach.[iii]

An alternative reality in a world of portable identity would be lifelong identities and fully shared reputations of who is trusted and who is not. Rather than trapping that information in private silos that must be recreated from scratch each time a new account is created for a user, the attestations supporting portable identity about the level of trust behind identities, without outing PII can and should live in public repositories as a public good.

PORTABLE IDENTITY AS DOING RIGHT THINGS RATHER THAN CONTINUING THE STATUS QUO

In a world of portable identity, trust is truly portable on the part of the individual rather than trapped within the silos of government or corporate databases. Rather than viewing the advent of such a “self-sovereign” notion as a loss of top-down power by national and corporate actors, centralized authorities might instead remember that they still control the level of permission granted by themselves to holders of portable identity. Privacy enhancing separation of private information from attestations about that information need not weaken the quality of risk and compliance decision processes. Quite the contrary – oversight is drastically improved with universal access to ever more complete and portable sets of attestations about identities that are in the bright transparency of a public ledger rather buried in dark silos.

NOTES

[i] The notion that persons would move around and not have their mobile phone with them has now become an edge case. Thus, rather than serve as just another method of logging into one's identity (i.e. as a special "mobile" case of access to the internet), an individual's particular mobile device has become the core (private/secure/trusted) method of access to the internet in an identifiable (yet portable) manner. As such, the notion of binding one's name, attestations, and privately identifiable information onto a single mobile device becomes foundational for the operationalized execution of portable identity. An encrypted backup of data may be in the cloud for restoration, but the practical day-to-day mechanism for creation, control, and carrying of identity resides within one's mobile phone.

Even persons without a mobile phone can have a globaliD by using a biometric attestation that can be established by a trusted agent as their marker for connecting to a balance or other permissions they may hold within the globaliD ecosystem

[ii] Control of the name reverts via a pre-designated chain-of-command to the top-of-the-list power-of-attorney. Upon revocation, the power-of-attorney instantly assumes control of the name in question on their phone. The name becomes a (temporarily) owned asset in addition to their already mobile phone based existing "root" name. And that power of attorney is, in turn, successively governed by their own delegated powers of attorney so that there is always a chain for further revocation and subsequent restoration that ensures no name is ever stuck in limbo without an authorized overseer.

[iii] The limits inherent in the current BSA/AML system, in which identity information is siloed by institution and geography, but transactions take place on a global level, are increasingly apparent. A recent United Nations study estimated that despite massive and costly KYC risk/compliance regimes and de-risking practices that exclude billions of persons from financial inclusion, 99.8% of money laundering activity currently goes undetected.