OMIDYAR NETWORK
A WORLD OF POSITIVE RETURNS

Point of View

Updated: October 2017

Digital Identity and Privacy

The Issue
Identity is vital to participate fully in our modern digital society and economy.

Yet, designed and implemented unchecked, digital identity technologies could have unintended adverse consequences for the world's most vulnerable populations.

Why Is Digital Identity Necessary?
The digital revolution of the 21st century is driving everyone to embrace technology to varying degrees. Access to and engagement with government, the private economy, our communities, and each other all increasingly rely on digital connection. And underpinning all these connections is the necessity to assert one's digital identity: a digital means of proving we are who we claim we are.

The growing digital economy will bring massive opportunities as connectivity increases and distance evaporates as a barrier for engagement and trade. Transactions will increasingly occur without the two transacting parties ever meeting. Access to state benefits and a range of other services have the potential to become easier, faster, and more inclusive.

At the same time, the digital economy will introduce new barriers to access and engagement for those who lack identification or are unable to establish identification for want of digital access. The World Bank estimates that there are more than 1.1 billion people in the world who lack the ability to prove their identity. For these individuals, many of whom already face social and economic exclusion today, inclusion in the rapidly digitizing world becomes even more difficult without the identifiers required to engage in it. But to ensure that digital identity is truly inclusive, secure, and safe for everyone to use, it requires a shared and thoughtful development of the necessary checks and balances.

HOW WE DEFINE DIGITAL IDENTITY

Digital Identity, in its simplest form, is a digital means of establishing we are who we say we are. There are at least three types of digital identity in use today:

a. *Identity issued by an identity provider*: There are both public sector and private sector identity providers. In the public sector, a state typically issues identification and uses it to recognize each person uniquely, to provide rights or entitlements. Private sector identity providers — such as banks, tech companies, etc. — can also offer digital identity for access to commercial services. In some cases, there may be crossover between the public and private sector identities and the access they can unlock.

b. *De facto identity*: There are also de facto identities or attributes that are created for us when we engage in the digital economy — our phone data, our search data, social media data, data about where we go or what we watch, or data from other smart devices we use. Increasingly, such information can be used to identify us — or something about us — reasonably accurately, either through our own self-assertions or through the assessments of third-party algorithms.

c. *Self-asserted and self-sovereign identity:* In contrast to the means of identity provided by an external party, there are also identities or personas that we create for ourselves in the digital world where we choose how to portray ourselves and the claims we make. This category also includes identities or personas that use pseudonyms or other approaches to obscure all or part of our formal "legal" identity, thereby presenting ourselves as we want to be seen rather than embracing an identity provider's definition. These identities are heavily oriented toward the preferences of a particular individual, but may offer claims that clash with those of established identity providers.

Our View

At Omidyar Network, our hypothesis is that digital identity can lead to empowerment only if it (i) puts the individual in control of her identity and (ii) is built with checks and balances to protect personal information of individuals. At the heart of our perspective, we believe in three foundational precepts about digital identity. Identities must:

1. be available and useful to individuals
2. be non-discriminatory and designed for inclusion, meaningful user-control, and privacy
3. provide for recourse and accountability for harms caused

For a digital identity system to achieve these objectives, we must consider both technical design and governance. In fact, in our view, the technical design can be more effective in protecting individuals than the legal privacy framework of a given country, given the difficulty of enforcing rights and having real recourse for individuals who may have their privacy violated.

There is a growing body of work on privacy, data protection, and identity principles. But more needs to be done. The enumeration of comprehensive and specific safeguards, permissible uses of digital identity and personally identifiable information, recourse and accountability, are all critical to ensure that engaging in the digital world can keep us all empowered, safe, and secure.

Some Key Characteristics of Empowering Digital Identity

(A) Technical System Design

1. **Informed, meaningful user consent and control**
   Identity systems should ensure an individual is:
   - aware of the use of her ID and its associated data trails
   - able to permission its use (or, conversely, deny its use)
   - able to opt out of its use even after permission has been granted, and to not be compelled to use it
   - informed and able to understand the decisions made through the use of her ID and related data, even those beyond the initial use case
   - able to have meaningful recourse in the event of violations
2. **Limited data collection and use, with a specified purpose**
   Identity providers must not collect more information than what is needed for a transaction or application. If providers wish to use the data in another way, they should return to the user for informed consent and providers should not share the data with another party unless the user has explicitly consented for them to do so.
3. **Privacy by design –** Privacy protections should be proactively embedded within the technical architecture in such a way as to prevent harm rather than relying just on legal recourse mechanisms and accountability. Privacy and user control should be the default setting and must be integral to the system without diminishing functionality. This includes minimal collection and disclosure of data, creation of use-specific identifiers to prevent sharing of data without explicit user consent, and data destruction to ensure the reduced risk of reuse and abuse.
4. **Security –** Identity systems should be designed to minimize vulnerability. They should be resistant to attack from outside as well as from being compromised from within, utilizing such things as strong cryptographic capabilities, layered access control, and other checks and balances.

5. **Openness –** The technology architecture of identity systems must be open, allowing for vendor- and technology-neutrality, and, importantly, interoperability across systems and geographies.

(B) System Governance

1. **Inclusion –** Simply put, anyone who wants a digital identity should be able to get one. Access should be available for any interested individual to enroll, free from discrimination or limitation. At the same time, there should not be compulsory participation in identity systems, nor should users be required to use just one identity mechanism — there must always be alternatives to ensure that there is no exclusion.
2. **Transparency –** Individuals should be able to access information about what is being collected about them and why, how that data will be used to make decisions, and informed of any change to that circumstance, including use for a different purpose or intent to share with a third party. Additionally, there should be transparency about the policies and the infrastructure of the system itself so that parties engaging with it understand its structure, safeguards, and mechanisms for recourse.
3. **Legal framework –** Privacy must be recognized as a fundamental human right. Laws must be framed to ensure the basic protections that come with the recognition of such a right. The legal framework must reflect a global understanding of some basic tenets of the appropriate use of digital identity and personal information. It must define the recourse and accountability mechanisms that become available to individuals.
4. **Recourse and accountability –** Individuals should have access to independent mechanisms for redress and recourse that are not excessively burdensome or costly. There should be clear roles and expectations governing the behavior of system administrators, including access limitations and policies that delineate the responsibilities and liability of those who interact with identification data in all its forms. Accountability should be enforceable through means such as staff training, complaint channels, audits, arbitration, lawsuits, and civil or criminal penalties.
5. **Independent oversight –** The management and use by public and private sector entities of personally identifiable information should be subject to independent administrative and judicial review. This is important to prevent the misuse of digital identities by all actors, including review and oversight of law enforcement agencies for unlawful surveillance.

Implications for Omidyar Network Engagement

We articulated the conditions and characteristics we would like to see in any ID system design. Conversely, we also explicitly assert that there are systems and circumstances under which we would simply refuse to engage or support the introduction of ID systems.

These circumstances would include:

- Systems designed primarily, or even secondarily, for surveillance purposes
- Systems that are not designed to be inclusive, or are designed for discriminatory purposes (e.g., to single out a given ethnic group)
- Systems in states without robust privacy legal frameworks in effect or on the immediate horizon
- Systems that significantly depart from the Principles for Identification for Sustainable Development

We also recognize that increasingly there will be private sector firms developing innovative solutions that build applications on top of these ID systems with a goal of empowering individuals.

Indeed, Omidyar Network has invested — and will continue to actively invest — in the most promising entrepreneurs in this space. But we recognize the tension between the business model and incentives of a firm and the considerations noted above. This is why we believe it is so important to combine sound technical systems, good policy frameworks, and architectures with built-in privacy and user control.

Looking Ahead

Working together through policy frameworks and technical system design, stakeholders must (i) create pre-emptive and responsive tools for safeguarding users against privacy violations, and (ii) establish legal frameworks and mechanisms for oversight and recourse in the event of misuse or abuse. While we have aspirational goals about the "normative," we will need to continually engage in shaping these frameworks in the coming years.