OMIDYAR NETWORK

Omidyar Network Unpacks Good ID

MAY 2019

Digital identity systems are becoming increasingly prevalent worldwide. Omidyar Network supports the issuance and self-assertion of such identities as a key enabler to empower individuals to engage in the modern economy and with the modern state. But we recognize that there are significant risks to such technologies and programs.

For three years, Omidyar Network has used the term "Good ID" to characterize the empowering forms of digital identity we would like to see in the world. Good ID is our normative framing for any digital identity system that prioritizes individual empowerment while ensuring adequate safeguards.

Specifically, Good ID is inclusive, offers significant personal value, and empowers individuals with privacy, security, and control. Good ID builds trust with transparency and accountability. Good ID seeks to address exclusion, discrimination, surveillance, consent, and other key issues of our time.

Good ID expands on the Principles on Identification for Sustainable Development and the Framework on Digital Identity for Africa, which guide the design and practice of issuing national digital identity. Each of these contain 10 principles that help governments, in particular, build empowering, effective, and efficient national digital identity systems and governance mechanisms. The other forms of digital ID—de-facto ID from data trails and self-asserted solutions—do not yet have a similar set of guiding principles. We believe all digital identity should all aspire to meet the standard of Good ID.

We believe all digital identity should all aspire to meet the standard of Good ID.

At Omidyar Network, we make catalytic investments in mission-aligned startups and nonprofit organizations to advance Good ID across the state-issued, de-facto, or self-asserted digital identity continuum.

Many have asked what we mean by Good ID. Here, we share our evolving understanding about design features and practices that lead to Good ID. We also call for more research and implementation of good technology, policy, and practice to further refine Good ID.

How would I know Good ID when I see it?

In our view, Good ID is a function of both good practice and thoughtful technology and policy design. We enumerate these in turn.

Practice

Transparent, accountable, and trust-building practices lead to Good ID. System planners, technologists, program managers, policy makers, and investors either build or erode trust with digital ID holders with every choice they make.

Trust in systems and institutions influences people's adoption and choices in digital identity programs. And in today's trust-deficient economy, there are many good reasons why a digital ID issuer would want to support Good ID—if not solely for ethical reasons, at least to mitigate risk and pursue new business opportunities.

Transparent, accountable, and trust-building practices lead to Good ID. Trust in systems and institutions influences people's adoption and choices in digital identity programs. And in today's trust-deficient economy, there are many good reasons why a digital ID issuer would want to support Good ID.

In practice, Good ID champions:

- Believe that individual empowerment, agency, and control must be the focus of any digital ID system
- Make and fulfill public commitments to include users, civil society organizations, media, and other stakeholders in the decision-making process and to protect their rights and interests
- Show radical transparency about the choices and decisions being made along the way, including policies, design and data sharing contracts, tenders, and protocols
- Use ethical and legal frameworks, scenario-based tools, feedback loops, research, and future-resilient tools to make informed decisions before and after systems are built
- Use open standards and open-source technology to facilitate future evolutions of the digital identity system, without dependency on one vendor
- Take accountability and provide simple and satisfactory recourse for grievances when unintended consequences arise
- Prioritize trust and user participation as some important proxies for good policies, technologies, and practices

Design Features

Thoughtful design features in technologies and policies lead to Good ID. Omidyar Network has prioritized five features because they apply to all forms of digital ID, support individual empowerment and equity, and provide an anchor on which to develop Good ID systems. Many of these perspectives were honed with the publication of the World Economic Forum's 2018 insight report.

1. PRIVACY

Privacy is a fundamental human right. We believe it is the obligation of both public and private digital ID issuers to ensure individual privacy. If privacy is missing or lacking depth, a digital ID system will not truly empower.

In October 2017, we published our initial point of view on the critical relationship between digital identity and privacy, asserting it as the master key needed unlock the full potential of digital identity.

In the original article, we showed how privacy can be protected by making appropriate design choices and establishing a robust governance framework.

For example, privacy features in technology and policy:

- Limit the amount of data collected,
- Give individuals the legal right to change how their identity information is used,
- Enable full disclosure of how identity data will be used, and
- Proactively notify individuals when privacy policies change.

Our point of view also notes that providing end-to-end encryption of content is a grossly inadequate way of addressing privacy concerns, and can lead to perverse incentives. Read "Digital Identity and Privacy" for more ways privacy-by-design can lay the foundation for Good ID.

Privacy is a fundamental human right. We believe it is the obligation of digital ID issuers to ensure individual privacy. If privacy is missing or lacking depth, a digital ID system will not truly empower.

2. INCLUSION

The foundation of Good ID is the principle of inclusion. Individuals want the opportunities that digital identities unlock; Good ID makes digital ID systems accessible and fair with inclusive practices and features.

Target 16.9 of the UN Sustainable Development Goals calls for "legal identity for all". Simply put, anyone who wants a digital identity should be able to get one, free from discrimination or limitation, from the country where they legally reside and the institutions they trust. At the same time, individuals should also have access to alternative means of identification and choices in how they identify themselves.

The foundation of Good ID is the principle of inclusion. Individuals want the opportunities that digital identities unlock; Good ID makes digital ID systems accessible and fair with inclusive practices and features.

Additionally, to include the most people, users must have confidence in the system's privacy; adding more individuals from marginalized groups to poorly designed digital ID systems that track their location or note their ethnicity or religion will only intensify their vulnerability. In such cases, it may be better not to have a digital identity at all.

We believe good digital identities must offer:

- Equal and fair opportunity for everyone to establish and use digital identities that they can use to authenticate themselves when needed or desired
- Limits to the number and type of situations when any digital ID is mandatory
- Alternatives when individuals wish to participate, but not use a particular form of digital ID
- Low barriers in establishing and using identities, such as requiring minimal data to register and authenticate
- Safeguards against discrimination, such as processing applications inconsistently among different ethnic groups, religions, and gender identities
- Mechanisms to manage unintended consequences, such as clerical or technology errors that exclude individuals who should be able to apply for and use digital ID, and remediation for any related harms

We believe Good ID is, in part, defined by having high, personal value for individual users. The amount of friction and vulnerabilities individuals experience in using their digital ID ultimately increases or decreases that value. Therefore, Good ID shouldn't be difficult ID.

3. USER VALUE

We believe Good ID is, in part, defined by having high, personal value for individual users. The amount of friction and vulnerabilities individuals experience in using their digital ID ultimately increases or decreases that value. Therefore, Good ID shouldn't be difficult ID.

We believe good design drives good user experiences, which in turn drives good user outcomes. When digital ID is useful in accomplishing the things individuals want to do most, such as securing a loan to open a business, it leans toward Good ID.

We believe good digital identities must offer:

- Access to a range of meaningful services
- Accurate and precise records, reflecting the users' preferred level of privacy
- Convenience in use, registration, and management

- Identification and authentication processes that are as straightforward as possible, with friction proportionate to the purpose or use case
- Interoperability and portability so that identities should work across services, sectors, and geographies while upholding security and privacy
- Avenues for startups to build customer-driven services on top of the identity stack and innovate to provide more value overtime

4. USER CONTROL

Building on this, Good ID is embedded with personal agency and the ability for individuals to control and manage their digital identities.

We believe good digital identities must offer:

- Transparency so individuals can see who is collecting and divulging their data, what data trails are forming as a result, how others are using and processing their information, and for what purposes
- Mechanisms for meaningful, informed consent related to each new purpose and before any identity data is shared with another party; these should be embedded in technology and process so individuals can choose and change who uses, and accesses their identity data; for how long and for what purpose; and have the ability to update and remove their data as needed
- Options for individuals to deny use of their identity, update records when identity information changes, and revoke their permission even after permission has been granted
- Alternatives when individuals wish to participate, but not use a particular form of digital ID or disclose identity information beyond what is strictly necessary
- Recourse in the event of regulatory violations and user grievances supported by clear, legal frameworks

Good ID is embedded with personal agency and the ability for individuals to control and manage their digital identities.

5. SECURITY

We believe privacy is not possible without security. Good ID makes transacting in a digital world safer by minimizing vulnerability.

We believe good digital identities must offer:

- Data integrity, including limits on the amount of data that is collected and stored as well as clear roles and expectations governing the behavior of system administrators and anyone else who interacts with identity data in all its forms
- Rigorous cybersecurity practices and defensible systems, such as layered access control, strong encryption, and audits, that evolve continuously to mitigate threats and block unintended or unauthorized access, disclosure, or manipulation
- Safeguards from breaches, corruption, or loss of personal data embedded in technology design, operational controls, and regulations
- Timely disclosure of breaches to all parties affected
- Public and private frameworks that embed an audit trail, assign responsibility, and provide for recourse in the case of a security leakage or breach

We believe privacy is not possible without security. Good ID makes transacting in a digital world safer by minimizing vulnerability.

Omidyar Network has prioritized these five features for the universal foundation they provide to all forms of digital identity. We believe an emphasis on privacy, inclusion, user value, user control, and security create the foundation for impact and mitigate many risks of digital identity.

We acknowledge that our normative framing will have to evolve with new thinking, new technology, new experience, and new societal expectations. And to fully realize digital identity systems that maximize the benefits and minimize the harms to individuals, we know we will need more inputs from a diverse community of experts. Thank you in advance for sharing your experiences and opinions with us.

Please help unlock the full potential of Good ID by sharing your learning, viewpoints, projects, events, and other resources on the Good ID online platforms—www.good-id.org and @GoodID.