GEORGETOWN UNIVERSITY | beeckcenter social impact + innovation | Digital Benefits NETWORK

DECEMBER 2022

What is Digital Identity?

The Digital Benefits Network's (DBN's) research on digital identity is focused on identity proofing and authentication practices in benefits programs, but these topics are part of the broader digital identity landscape. In this short resource, we provide an introduction to the term and an overview of core questions related to digital identity.

Defining Digital Identity

The precise definition for digital identity is murky, as the National Institute of Standards and Technology (NIST) points out in their 2017 publication, *Digital Identity Guidelines*. In this work, NIST defines digital identity as "the unique representation of a subject engaged in a transaction." However, they also note that digital identity is "the online persona of a subject," and that a subject might represent themselves online in multiple, distinct ways.

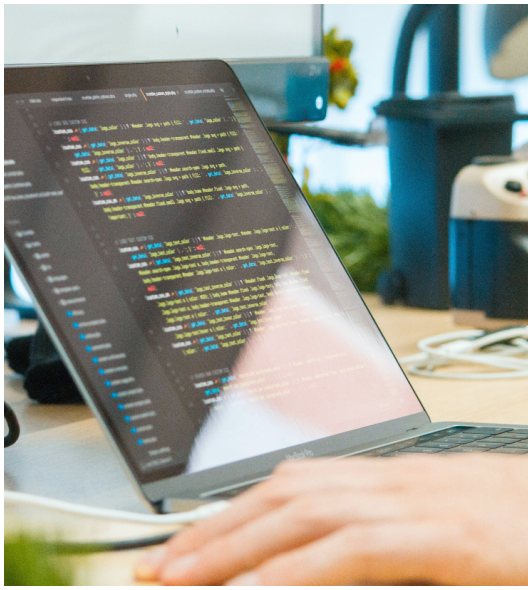
To put this in context, digital identity is sometimes used to describe the full sum of a person's online activity and information they have shared on the internet. This may include:

+ Usernames
+ Passwords
+ Search history
+ Personal identifiable information (PII) such as name, date of birth, address, etc.

Contributing Author

Elizabeth Bynum Sorrell
Researcher,
Digital Benefits Network,
Beeck Center for Social Impact + Innovation

But digital identity can also describe a specific online representation. For example, when a person wants to access online services such as a bank account or government application, they may be asked to create a specific digital identity or identifier including a username, to log in.



A digital identity is typically verified and confirmed using distinct processes of identity proofing and authentication. Identity proofing typically happens when an individual accesses a service or system for the first time. It allows a service provider – whether a bank, a government agency, or another entity – to determine whether the person creating a new account or applying for benefits is who they claim to be.

Once an individual has established a username or other login credentials, they might have to use authentication processes such as entering a password, biometric validation like Apple's Touch ID, or inputting an authentication code received via text message to confirm that they have access to an account. They may be asked to do this each time they want to use the site or service.

Discussions of digital identity also often highlight efforts to create digital identification credentials or digital IDs. This entails digitizing an existing physical identity credential or creating a new, fully digital identification system. Examples of this include state mobile driver's license projects, such as Colorado's Digital ID, or government-backed digital identification systems such as India's Aadhaar program, which issues unique, 12-digit identification numbers linked to biometric data. This data is then used to access services. (To read more about key terms in the digital identity space, check out our glossary of digital identity terms.)

Key Topics and Debates

Emerging approaches to digital identification and authentication technologies offer benefits and risks. This tension is illustrated through real-world examples including government-backed digital identification systems, mobile driver's licenses, and facial recognition technologies.

Estimates suggest more than one billion people lack identity documentation, and government-backed digital identification systems have been touted as tools for development that can help address this global identification gap. But such systems have been labeled as threats to privacy and human rights. Writing about the Aadhaar identification system in India, academics have raised concerns about how data from digital ID systems may be exploited in unexpected ways and create new forms of exclusion for citizens who are unable to successfully register, rather than promote inclusion or reduce corruption.

Media stories have also highlighted how technological issues in India's identity system can lock people out of needed welfare benefits with devastating consequences. Technologies, including distributed ledger technologies such as blockchain, could give users more control over their identity information. However, social science researchers argue that models of self-sovereign identity and distributed ledger technology are not inherently empowering, and have the potential to create and maintain bureaucratic and commercial power over individuals. Depending on implementation, surveillance and exclusion are potential risks if and when digital identification systems become entry points to essential services.

In the U.S., mobile driver's licenses have been framed as tools that may enable consumers to easily use government-backed credentials online. At the same time, experts highlight the potential for these digital IDs to exclude individuals who don't have device access and create new pathways for surveillance and tracking.

Facial recognition technologies (FRT) can be used for identity proofing and passwordless authentication, but the use of FRT raises questions about privacy, data security, and surveillance. These questions include:

+ Who has access to facial images?
+ How is that data stored and used?
+ How long is this type of data held?

When information like a password or username leaks in a data breach, it's possible to change it. However, it may become more difficult to re-secure your private data if leaked information includes biometric data, like facial images.

FRT deployment can also pose an equity problem. A National Institute of Standards and Technology study and independent academic research have demonstrated biases in commercially-available facial recognition algorithms. These tools are less effective at appropriately identifying faces of Black, Asian, and Native American individuals. Consequences for false positive or false negative outcomes can be serious. In a law enforcement context, a false positive – the wrong person is deemed to be a match – can lead to a wrongful arrest. In the context of benefits applications, a false negative may mean an eligible applicant is denied assistance.

Balancing the Need for Identification and Risks of Harm

A central tension in debates about these technologies is the tradeoff between necessary forms of recognition and identification, for example to access services, and the risks for surveillance and misuse of personal and private information.

For benefits programs and other government services, digital identity solutions have to balance verification requirements and fraud prevention against accessibility and usability for the populations they serve. Effective, equitable implementation of new identity technology may be facilitated through design justice approaches that engage and incorporate user experiences, and clear data protection standards.

In our research on digital identity in public benefits, the DBN seeks to identify and amplify approaches that are effectively negotiating these tensions to promote equitable benefits access and reduce disparate impacts. You can read more about digital identity on the Digital Benefits Hub, and find our other introductory resources including:

+ A glossary of digital identity terms,
+ A primer on digital identity in public benefits,
+ An overview of the federal government's digital identity activities.

Agencies or individuals interested in our research on digital identity can subscribe to the DBN and follow our updates. If you would like to discuss our research further or are interested in sharing your own experiences administering identification and authentication processes in a benefits program, we encourage you to reach out to us at digitalbenefits@georgetown.edu.

Get in Touch

Our Digital Benefits Network team is here to help!

Visit us at the Digital Benefits Hub

Please contact us with any thoughts, questions, or potential collaborations via email at digitalbenefits@georgetown.edu