Americans Need a Digital Identity System, Stat!

Waldo Jaquith
State Software Collaborative, Georgetown University's Beeck Center

"Can I see your ID?"

How many times have you heard that simple request? Most of us automatically pull out a driver's license. But if you don't have a driver's license, proving who you are in America can be complicated. As more of our lives and interactions move online, it'll take more than pulling out a driver's license to create an effective digital identity proofing system. Meeting that challenge is foundational for a healthy, equitable, well-functioning society and economy.

The COVID-19 pandemic shined a spotlight on the need for an effective digital identity system in the United States. As the pandemic hit, millions of desperate Americans went online to apply for public benefits—unemployment insurance, SNAP and EBT food benefits, PPP, and housing and rental assistance—and found they were delayed or denied payments because of problems verifying their identities. At the same time, criminals were successfully using stolen identity data to defraud these government programs of billions of dollars.[1] The urgency has never been greater to find the right balance between providing easy, equitable, and timely access to benefits to those in need and preventing fraud.

Nearly every interaction people have with government begins with proving their identity—voting, attending school, accessing public benefits, getting a vaccine, collecting Social Security, and entering or leaving the country. Countless commercial interactions also require a government-issued photo ID—opening a bank or credit card account, cashing a check, going to the emergency room, getting a job, signing a lease, renting a room, buying a beer, or riding on a plane.

Proving who you are in the United States is complicated, because there is no single, definitive way for people to prove their legal identity. The default is a state-issued driver's license, federal employee ID, military ID, passport, or green card. But for the poor—or poorly connected—going through the process to get an official ID presents significant barriers. Eleven percent of Americans lack a government-issued photo ID, a group that disproportionately includes senior citizens, African

The Community Development Innovation Review focuses on bridging the gap between theory and practice, from as many viewpoints as possible. The goal of this journal is to promote cross-sector dialogue around a range of emerging issues and related investments that advance economic resilience and mobility for low- and moderate-income communities and communities of color. The views expressed are those of the authors and do not necessarily represent the views of the Federal Reserve Bank of San Francisco or the Federal Reserve System.

[1] Dena Bunis, "IRS Warns Consumers of Stimulus Check Scams," AARP, April 2, 2020, https://www.aarp.org/money/scams-fraud/info-2020/stimulus-checks-scams.html.

Americans, Latinos, and people making less than $25,000 per year.[2] In fact, one in four Black adults have no current government-issued photo ID.[3]

Given the confused and fragmented state of basic identity verification in the United States, it's no surprise that proving an individual's digital identity is even more fraught.

Why Digital Identity Matters

When a member of the public needs to apply for public benefits, identity verification is the first, indispensable step. It confirms both that a person exists and that the applicant is that person (or is authorized to represent that person).

During the pandemic, as the majority of government and commercial services have moved online, identity verification also needed to become digital. Pre-COVID, benefits programs and financial institutions could rely on people coming into their offices and showing a government-issued photo ID, but the pandemic rendered that impossible. That meant that applying for any sort of public benefit—unemployment insurance, SNAP, emergency rental assistance, PPP loans, COVID testing, COVID vaccinations, or obtaining new commercial products—all required digital identity verification.

There is no national standard for digital identity, no common set of practices, no dominant vendor, and until spring of 2020, it was rare for agencies to have any digital identity verification tool whatsoever. The combination of these lax digital identity practices and the COVID-induced reliance on digital services meant that 2020 saw both dramatic delays in determining eligibility for benefits and growth in fraudulent benefits applications, with billions of dollars lost to crime rings. The United States has so far discovered $36 billion in fraudulent COVID benefits claims as a result of inadequate digital identity infrastructure, and that number will only go up.[4] The bulk of application backlogs under COVID resulted from digital identity problems, delaying getting much-needed benefits to millions. This is, of course, a terrible waste of tax dollars, but it also undermines trust in government and the financial system, and prevents money from getting to those in need.

How Digital Identity Works Today

The identity process in the United States is fragmented—unlike most countries, we have no national identity card, and instead leave that to states. Things are worse still for digital identity, where government agencies and commercial entities labor under a privatized, fragmented identity-verification marketplace.

[2] Brennan Center for Justice, "Citizens without Proof: A Survey of Americans' Possession of Documentary Proof of Citizenship and Photo Identification," Voting Rights & Elections Series (New York: Brennan Center for Justice at NYU School of Law, November 2006), https://www.brennancenter.org/sites/default/files/legacy/d/download_file_39242.pdf.

[3] Ibid.

[4] Greg Iacurci, "Scammers Have Taken $36 Billion in Fraudulent Unemployment Payments from American Workers," CNBC, January 5, 2021, https://www.cnbc.com/2021/01/05/scammers-have-taken-36-billion-in-fraudulent-unemployment-payments-.html.

Although most of the underlying documents and data needed to prove you exist (e.g., birth certificate, Social Security number) and that you are you (e.g., passport) are generated and "owned" by some government entity, those data are highly fragmented and spread among federal, state, and local agencies, and not easily shared. Compounding the problem, public agencies often augment government data sources with private data sources (banks, credit agencies, phone companies), which adds another layer of cost, complexity, and time.

In the private sector, a robust market for automated commercial digital identity proofing services has developed to support banks and financial service companies that are required to know the real identity of their customers in order to comply with "know your customer" (KYC) guidelines and anti–money laundering laws.

Like the government, most of these vendors employ a similar model, linking data about a civil identifier (such as a driver's license or a Social Security number) with personal data, such as addresses, from credit agencies and commercial data aggregators to verify personal identity. Verification often involves multiple-choice questions about credit history (e.g., "How much was your income in 2018?"). If the verification process is successful, the vendor's software informs the agency of that, allowing the applicant access to agency services. Sometimes this is paired with having applicants send a photo of their government-issued photo ID and a photo of themselves, with the photo of the ID serving as a sort of a crude digital ID and the selfie serving as evidence that they're the legitimate holder of that identity card.

As with government-issued photo IDs, there are disparities in who has a sufficient data footprint to have their identities verified in this manner. These "credit invisibles," as the Consumer Finance Protection Bureau terms those who do not appear in the nationwide credit reporting agencies' databases, comprise 11 percent of the adult U.S. population.[5] As with government-issued photo IDs, some demographics are again over-represented: African Americans, Latinos, and residents of low-income neighborhoods. In fact, 30 percent of residents of low-income neighborhoods have no credit record and are consequently unidentifiable via most existing digital identity processes.[6]

Government's role in this process is to act as the source of truth about what people exist within the United States, via birth and death records, driver's licenses, passports, and related methods of uniquely identifying individuals. Agencies generally employ security, privacy, data use, and interoperability regulations and frameworks to both promulgate and protect those records. There is no national, standardized system for normalizing, matching, and deduplicating these records, and there is no agency charged with oversight of this informal national identity system.

The private sector's role in this process is, quite simply, to intermediate the government's own data and sell them back to the government again, as an identity-proofing process. This is because these data aren't possessed by "government," but instead by a series of unrelated government agencies that have no practical capacity to share or aggregate that data. Absent any incentive to do otherwise, this collective-action problem leaves agencies with no option but to buy back their own data.

[5] Kenneth Brevoort, Philipp Grimm, and Michelle Kambara, "Data Point: Credit Invisibles" (Washington, DC: Consumer Financial Protection Bureau, May 2015), https://files.consumerfinance.gov/f/201505_cfpb_data-point-credit-invisibles.pdf.

[6] Ibid.

Problems with Privatized Digital Identity

This existing system has some obvious flaws.

Government's providing data to the private sector and then buying them back again is clearly extremely inefficient. The data being purchased back aren't even improved; they've simply been turned into a service.

In relying on private vendors, government is engaging in an online practice that it would not engage in offline. An applicant coming to a physical office needs to provide a government-issued form of identification, not a private-sector–issued form of identification, and it's puzzling that government would use a lower standard for Internet-intermediated transactions. If anything, online application processes should have a higher threshold for identity verification, since they're easier to defraud at scale—one person's capacity to steal others' identities online is virtually limitless, while there is a limit to the number of disguises and fake IDs that a person can procure.

Government handles identity risks in the same way that it deals with risks around software. One reason that government agencies prefer to rely on outsourced Software as a Service (SaaS) for technical needs is that it provides an illusion of security, because the security is theoretically the vendor's problem. When government owns and operates its own technology stack, it's obliged to take it through an extensive security review process; this process is far simpler for SaaS. The security hurdles required for government to set up its own identity verification system are significant and expensive, but by leaving this work to a comparatively lax private sector, government is paying far more via the criminal exfiltration of vast sums of money from benefits programs.

Outsourcing digital identity has the effect of isolating government from the impact of false negatives. If people are denied benefits because a digital identity vendor cannot validate them, not only might they simply give up and never receive their benefits, but the vendor is likely to chalk that up as a successful block of fraudulent applicants. Given the demographics that are unlikely to have a government-issued photo ID and that are likely to be "credit invisible," the very people who are likely to have a hard time claiming benefits are the people least likely to have any other kind of safety net to fall back on. The result is a social safety net that too often fails those it claims to serve.

The government may be best positioned to run a more comprehensive system, because its incentives are more aligned with citizens. No matter how much data they collect, commercial companies can never replace the government's important role in establishing a person's legal identity, whether in person or online. Equal access for all, accountability, privacy, and security are mission-critical features. Unlike the government, commercial providers have no obligation to serve everyone or even stay in business. One of the major vendors in this space, Equifax, failed to protect the vast quantities of data it had collected about people without their permission, leading to extensive personal data of about 147 million Americans being stolen. [7] The only recourse available to victims was signing up to receive a settlement from a class-action payment; there was no option to vote the president of Equifax out of office, no agency secretary for Congress to call in to explain how

[7] Federal Trade Commission, "Equifax Data Breach Settlement," January 2020, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.

they allowed this to happen. So, beyond the financial inefficiencies of taxpayers' paying commercial vendors over and over again to be intermediaries of government-generated data and the increased risk of a fragmented system of data collection and transfers, the risk of outsourcing this important job opens a Pandora's box of risk to the individuals who need access to government services.

Another risk of reliance on private vendors for identity verification is the potential for government to be cut off from essential citizen data. The United Kingdom maintains a digital identity system that is federated out to private vendors. One of those vendors, Experian, declared in February 2021 that it was getting out of that business the following month, leaving 2.1 million people needing to re-register.[8] This left the U.K. government at a loss, since security restrictions prevent it from identifying which registrants have their identities stored on Experian's system. Experian, of course, has no obligation to remain in a particular line of business, or even to continue to exist.

Finally, market fragmentation means that people need to maintain a series of different accounts for various government services, each of which is likely to use different data sources and metrics for evaluating identities. This leaves governments paying multiple competing vendors for duplicate records, it leaves people with multiple accounts with different vendors, and it leaves applicants puzzled about why they can validate their identity for one public service but not another. Each new vendor in this space is yet another digital identity that members of the public are obliged to keep up to date, which collectively serves as a sort of cognitive tax; the more public services that somebody requires, the greater that tax. This approach places the greatest burdens on the people who are in the worst position to shoulder them.

The dream of state benefits programs is to have an integrated eligibility system, so that applicants' eligibility can be determined once and applied across benefits programs. Fragmentation of identity across vendors moves states further from that goal, which instead requires persistent, unified identity.

Improving Digital Identity

How could we do digital identity in a better and more inclusive way?

There is, happily, a simple way to fix many of these problems: soup up Login.gov, the federal government's existing digital identity service. A product of the General Services Administration, Login.gov provides a single sign-on that can be used across government agencies and complies with the National Institute of Standard and Technology (NIST) IAL2 identity-proofing standards. The program dates to 2017 and promotes itself as "the public's one account for government." It currently licenses Equifax's data for its identity-validation process. Its customers include the Department of Defense, the Small Business Administration, and the Department of Homeland Security, for which it maintains digital identities for nearly 30 million Americans. Login.gov's customers are currently all federal agencies, because it was not permitted to sell its services to states until late 2020.

[8] Lis Evenstad, "Experian to Close More Than Two Million Gov.Uk Verify Accounts," ComputerWeekly.com, February 9, 2021, https://www.computerweekly.com/news/252496069/Experian-to-close-more-than-two-million-Govuk-Verify-accounts.

The circumstances of Login.gov's creation require it to be a cost-recoverable service—that is, it has to charge agencies for each user of the system. Given that we now know that fraudulent digital identities are a vector for stealing billions of dollars from public coffers, the logic of "cost-recoverable" indicates that it's well worth fully subsidizing Login.gov for every federal, state, and local agency that wants to use it. The program is run by fewer than 40 people—a relatively small appropriation would have a vast return on investment.

Expanding access to the Federal Data Services Hub (Federal DSH) would be another smart investment. Housed at the Centers for Medicare & Medicaid Services, the Federal DSH uses a variety of government and commercial data sources to verify identity and other information, such as address, income, and employer information for individuals applying for health insurance on a state or federal health exchange.[9]

By integrating and expanding access to the existing federal services offered by Login.gov and the Federal DSH, individuals would no longer need to maintain a series of accounts for each separate agency or government service and could instead create a single government login that unites all of their interactions with government. This unified identity system could be used to create efficiencies, prevent fraud, and support a broader unified public benefit system for people to access health care, food, or unemployment benefits. Login.gov's use of industry-standard authentication protocols means that private-sector companies could be permitted to validate individuals' identities using their Login.gov account, a virtual equivalent of showing a government-issued photo ID to get into a bar or buy a prescribed controlled substance from a pharmacy.

Conclusion

Government's inability to deliver much-needed services to the public during the pandemic and disparities in access for communities of color can be traced back to its failure to adopt an effective digital identity proofing system. The lack of an effective system has also contributed to the fragmented private system of data collection and transfers to confirm identity, directly impacting financial services and financial inclusion.

The practical approach to meeting this challenge involves clear guidance and standards, cross-agency and intergovernmental coordination, close collaboration with private companies, and expanding access to existing federally owned platforms, such as Login.gov and the Federal DSH.

Reshaping the currently fragmented marketplace of digital identity tools won't happen overnight, but a government-supported centralized digital identity proofing process that provides an automated, secure, and interoperable system that is accessible to all, inclusive, and protects personal privacy is fundamental for a healthy, well-functioning society and economy. This kind of system would be fundamental for providing essential government services and has the potential to further support innovation and access in financial services.

There is no time to waste.

[9] Joel Winston, "The Billion-Dollar Technology Stack Powering Obamacare," Medium, April 21, 2017, https://medium.com/@JoelWinston/the-billion-dollar-technology-stack-powering-obamacare-929114c3be0e.

Waldo Jaquith *is a technologist with extensive experience in the government, non-profit, and for-profit sectors. He works for the State Software Collaborative, housed at Georgetown University's Beeck Center. Until recently, he worked for 18F, the federal government's technology shop, developing and promoting best practices for procurement of custom software. Previously, Jaquith worked for the White House Office of Science and Technology Policy under President Obama. He lives near Charlottesville, Virginia with his wife and children.*