SOFTWARE CO-OPS AND DIGITAL IDENTITY

How U.S. State and Local Governments Are Adapting Login.gov To Verify Identity

October 2021

By Waldo Jaquith

beeckcenter
social impact + innovation

ABOUT THE BEECK CENTER FOR SOCIAL IMPACT + INNOVATION

Based within Georgetown University, the Beeck Center brings together students, expert practitioners, and extended networks to work on projects that solve real-world challenges using data, design, and technology as instruments for equitable societal change. Through the actionable research and tools we develop, the communities of practice we build, the policies we amplify and advocate for, and the skills and pathways we invest in, we strive to equitably improve the systems we rely on in daily life.

ABOUT THE STATE SOFTWARE COLLABORATIVE

The Beeck Center's State Software Collaborative is bringing together U.S. software cooperatives to facilitate their development of shared software and services. Instead of 50 states buying 50 versions of near-identical, overpriced software, we're facilitating the cooperative development of high-quality, fair-priced software to be shared among agencies.

ABOUT THIS DOCUMENT

This project was supported by Flourish Ventures and builds on a larger body of work exploring state software collaboratives as means to better share common code for state government service delivery.

The United States needs a national strategy for verifying identities for online interactions with government, and it would do well to adopt and amplify the existing, proven processes created by interstate software cooperatives.

Background

Americans' interactions with government often begin by proving their identity. Registering to vote, passing through an airport's TSA checkpoint, applying for SNAP benefits, getting a marriage license, interacting with the DMV, and any of dozens of other common activities require that the person prove that they are who they claim to be. This is a long-standing fraud-prevention practice, as accepted as it is common. The gold standard for proof of identity is a government-issued photo ID—most commonly a state-issued driver's license, although it may also be a military ID, a government employee ID, a passport, a tribal ID, or a green card, among other types

Proving identity requires two basic steps: demonstrating that a given person exists, and then proving that the claimant is that person. The former is comparatively easy, the latter is comparatively hard. A state driver's license establishes that the identified person actually exists, and the license includes information to allow a third party to visually determine whether the bearer is actually the identified person, by including the identified person's photograph, eye color, height, weight, address, and signature. In this way, somebody can show a state driver's license to a government employee, who can use that to verify that the person standing before them is the same person who previously had their identity rigorously verified by the state's motor vehicle agency.

THE IMPACT OF COVID

This system worked relatively well until the onset of the COVID-19 pandemic in March 2020. Suddenly, interactions with government were intermediated by telephone and the internet, which provided no mechanism for people to display a government-issued photo ID. A process that was created for in-person interactions was useless for remote interactions. Just when millions more Americans needed unemployment insurance benefits and welfare benefits, there was no infrastructure to allow them to clear the very first hurdle of proving their identity.

Desperate state agencies turned to private-sector identity-proofing vendors to clear their backlog of benefits applicants. Agencies no longer verified identities, but instead paid companies to verify identities on their behalf, and report back to the agency with a "verified" or "not verified" for each applicant. How did these companies do it? Generally by automatically turning the applicants' credit records into a quiz, prompting the applicant to answer multiple-choice questions about themselves, such as "what bank provided your 2016 auto loan?" or "what was your monthly mortgage payment in 2019?" The theory is that only the real James R. Garcia of Boise is likely to know the answers to these questions about James R. Garcia of Boise.

Some vendors used an alternate model, in which an applicant submits a photo of their driver's license or passport and a selfie, and the vendor compares the two on behalf of the government agency. Dozens of vendors sold these services to local, state, tribal, territorial, and federal agencies, often on sole-source contracts awarded hastily to meet the unprecedented need, inserting themselves as a new layer between government agencies and the public that they serve. In these use cases, the person's claimed identity is valid because the vendor says it is.

This approach is curious when compared to in-person identity verification. In person, if somebody displays a photo ID provided by a private company, they cannot expect a government agency to accept that as proof of identity. Government did not control the circumstances under which that photo ID was provided, so they cannot confirm that it is legitimate. There is no reason why internet-intermediated government interactions should be subject to different rules than in-person interactions.

LOGIN.GOV

The U.S. federal government operates a centralized login and identity-verification service: Login.gov. Managed by the General Services Administration's (GSA) Technology Transformation Services, this cost-recoverable service dates to April 2017, when it was created in a joint effort between GSA's 18F and the White House's U.S. Digital Service. This cloud-hosted service is available only to government agencies, charging on a per-user basis. There are onerous security requirements that accompany housing user accounts, and the attraction of Login.gov is that agencies can meet those obligations by having the login service handle them.

Most of Login.gov's business is housing non-authenticated user accounts—basically just usernames and passwords, without any need to verify that the account holder is actually any particular person. But, for an additional per-user fee, Login.gov will verify the identity of each user. Their identity verification process uses an array of data sources to verify the user's identity, using attributes that may include the person's name, Social Security number, address, phone number, date of birth, and a photo of their state-issued ID card. Those user-reported values are then verified through data sources including driver's license databases, phone records, and credit agencies. When necessary, addresses can be verified by sending an authentication code to the user's reported postal address.

Note that Login.gov does not offer standalone identity verification as a service (IVaaS), but only as an additional step in the registration process. For an agency to benefit from Login.gov's IVaaS, they must replace their existing authentication system with a full Login.gov integration.

Login.gov's customers include the Department of Defense, the Small Business Administration, and the Department of Homeland Security, for which it maintains digital identities for more than 30 million Americans.

Login.gov was created for federal agencies, but in late 2020 they were given limited permission to experimentally provide service to state agencies.

THE PROBLEMS WITH OUTSOURCING

There are significant inefficiencies under this private-sector model that took off during the pandemic. Vendors generally sell their services to individual state agencies, rather than to entire states, resulting in states paying repeatedly for near-identical or even identical services.

This fragmented marketplace also leaves people managing multiple digital identities from various vendors. For example, people who become unemployed often require services from a series of agencies (unemployment benefits, subsidized health insurance, child care, food assistance, etc.), and each one of those agencies may well require creating a new digital identity with a different identity vendor in order to qualify for benefits. An applicant may find that their identity can be verified by one vendor, but not by another. They need to keep track of usernames and passwords for all of the services that they're required to use, and that's in addition to their accounts on the agencies' websites. Years into states' efforts to create "integrated eligibility systems"—a single, cross-agency benefits application process—this new complexity constitutes a significant step backward.

Inserting a constellation of private businesses between the public and government agencies is a seismic change in government service delivery that should not be entered into lightly. As long as government has existed, it has interfaced directly with the public that it serves. This new model puts a layer of private enterprise in the middle of that relationship, sometimes just for the moment of verification, but sometimes permanently. The crucial data of which digital identities map to which verified identities will be fragmented across vendors, rather than living within government where it could be reused for identity verification over and over again at no additional cost. It is inevitable that vendors will raise their rates, go out of business, fail to protect individuals' data, etc., and many agencies have no control over whether they can continue to have direct access to the members of the public who they serve.

Identity verification is really a service and a product: the service of verification, and the product of a verified identity. The service is valuable, but the resulting database of verified identities is far more valuable. When government pays for verification, and then doesn't own the resulting database of verified identities, it is making a capital investment in a private business that is using that product as a wedge to drive between government and the public.

Finally, this approach poses a basic security problem. In 2017, consumer credit reporting agency Equifax announced that the data they'd collected on 148 million Americans had been stolen in a massive data breach. That's the very data that's used to verify identities under most private online identity-verification systems. (In fact, Equifax is a vendor of identity-verification services to government.)

In a May 2019 report by the U.S. Government Accountability Office ("Federal Agencies Need to Strengthen Online Identity Verification Processes"), the agency concluded that this ostensibly private personal information is now so readily available to criminals that it's no longer of any value in verifying identities. Also, individuals' credit records are accessible by a broad array of companies, ranging from debt collectors to landlords, making it easy to obtain a list of answers to these ostensibly secure identity verification questions.

The Present Need

COVID-19 moved government service delivery online, and there's every reason to believe that move is permanent. In-person service delivery will resume in time, but the default delivery mechanism will now be internet-intermediated. Government is now unavoidably in the identity-verification business, because doing so is central to delivering on agency missions.

The United States needs a national strategy for securely verifying identities for online interactions with government. The simplest way to do this is to emulate the existing physical ID system, which is a largely federated process controlled by states. The American identity system is the product of a century of laws, regulations, rules, norms, political bargains, and infrastructure. A near-term viable online identity-verification system must confine itself to those limitations.

State and Local Use of Login.gov

Today, no state or local agencies are using Login.gov, although not for lack of trying. After years of effort, Login.gov was given permission to sell its service to state governments in late 2020. Significant limitations were put on that ability, though. The White House Office of Management and Budget's memo authorizing sales to states urged caution, calling for a "measured approach" to the expansion. The GSA's Office of General Counsel, in turn, interpreted this as restricting Login.gov to selling "pilot" services to state agencies, limited to a one-year duration of services, and to no more than six states: two small-population states, two medium-population states, and two large-population states.

In the months since that guidance, dozens of states' agencies have expressed interest in adopting Login.gov, but none have been willing to accept the terms. The term "pilot" has a reserved meaning to some types of agencies, meaning a disposable experiment that could disappear at any moment. Even the best-case scenario of a year of service does not justify the work required to transition to (and then away from) Login.gov. The switching costs are too great for a one-year term.

Another limitation on uptake, albeit a less important one, is that identity verification is a component of Login.gov, and not a separate service. For a state agency to use Login.gov's identity verification service, they must also replace their login system, which is a significantly more invasive process than mere identity verification.

There is reason to think that Login.gov will soon be markedly more viable for states. Robin Carnahan was sworn in as the GSA administrator in July 2021 and has long prioritized shared software. Administrator Carnahan co-founded the State Software Collaborative as a Beeck fellow in 2020, and has already signaled an intent to support Login.gov's expansion to state and local governments. GSA has received significant amounts of new funding under the American Rescue Plan, some already earmarked for the Technology Transformation Service, the department overseeing Login.gov.

State Cooperatives' Identity Data

Since the 1960s, intergovernmental software cooperatives have quietly underpinned and facilitated the operations of government throughout the United States. These organizations are made up of two or more agencies, jointly supporting the development of software for their collective use, operating under some kind of a governance structure. Today there are many dozens of intergovernmental software collaboratives providing the software that operate DMVs, highway departments, libraries, labor agencies, insurance commissions, and transit agencies, for example. These are often housed at long-standing non-profit organizations that coordinate the interests of these agencies. (For more about intergovernmental software cooperatives, see our April 2021 report, "Sharing Government Software: How Agencies are Cooperatively Building Mission-Critical Software.")

Much of the infrastructure for digital identity verification has already been implemented by a trio of existing, national interagency software cooperatives: the American Association of Motor Vehicle Administrators, the National Association of State Workforce Agencies, and the National Association for Public Health Statistics and Information Systems. These organizations are each nearly a century old, and have all been coordinating their respective state agencies for that entire time. A combination of what these co-ops already do provides a framework for a national, federated digital identity verification system. The United States would do well to adopt and amplify these existing, proven processes created by interstate software cooperatives.

AMERICAN ASSOCIATION OF MOTOR VEHICLE ADMINISTRATORS

The American Association of Motor Vehicle Administrators (AAMVA) is a non-profit organization established in 1933 to standardize driver's licenses between states. Their members include all 50 states, Washington D.C., and the U.S. Virgin Islands (plus Canadian territories and provinces). They provide 18 different shared technology services for state motor vehicle agencies, including on-premises software and software as a service (SaaS). The bulk of that software facilitates exchanging driver, vehicle, and identity information between state agencies.

AAMVA's major offering in this space is their Driver's License Data Verification (DLDV) application programming interface (API). It's used to verify that the data on the card matches the data held by the jurisdiction that issued the document. A query to the DLDV is passed along to the issuing state in real time, which reports whether each data field on the card matches or doesn't match (e.g., the name is the same in the state database as on the driver's license, but the date of birth is different). The DLDV is open for use by private vendors, for a fee. AAMVA also provides a series of identity verification services that are wrappers for other services, including Verification of Lawful Status (Department of Homeland Security's Systematic Alien Verification for Entitlements), U.S. Passport Verification Services (Custom and Border Patrol Protection System, which has a copy of the Department of State's passport records), and Social Security Online Verification (SSA). Each of those services could be connected to and queried individually, but AAMVA recognizes the value of unifying identity services behind a single interface.

Login.gov uses DLDV as part of their identity-verification process.

Looking ahead a bit, things get really promising with AAMVA's Mobile Driver's License work. They've coordinated U.S. work on the under-development international standard for mobile driver's licenses, ensuring that motor vehicle administrators can support them. The idea is to replace physical driver's licenses with software-based licenses on mobile devices, protected by device-level biometric verification. This will allow people to virtually present an identity for themselves and to verify, to the state's satisfaction, that they are that person. It's the online equivalent of showing a government-issued photo ID. Fifteen states are testing digital driver's licenses, and Apple recently announced they're incorporating mDL support into iOS in collaboration with eight of those states, but it will be years until the standard is broadly adopted by states and usable to prove identity online.

AAMVA is uniquely positioned to lead a transition to a federated, state-led digital identity system, whether via its existing Driver's License Data Verification API or its new digital driver's license standard. Any federated identity verification service must inevitably lead with integration with AAMVA's services.

NATIONAL ASSOCIATION OF PUBLIC HEALTH STATISTICS AND INFORMATION SYSTEMS

The National Association of Public Health Statistics and Information Systems (NAPHSIS), which dates to 1933, represents and connects every U.S. state's vital records office. They operate a service—Electronic Verification of Vital Events (EVVE)—that provides lookup services to answer the simple question of "is this person alive?" NAPHSIS doesn't store any of this data themselves, but instead routes requests directly to each state's system, which checks their birth and death records and returns a result in real time. Forty-nine states provide birth and death records via EVVE, and the great majority of states participate in EVVE's "Fact of Death" system, which can review a list of identity records and flag those that are known to be deceased.

Birth and death records are pillars of any digital identity system. The presence of a birth record can be used as evidence of an individual's existence, and the presence of a death record can be used as a sign of fraudulent activity. NAPHSIS's EVVE is the sole source of this information. There is no other API or service that aggregates this information. The customers of EVVE include the Social Security Administration, the Office of Personnel Managements, many Departments of Motor Vehicles, the Department of Homeland Security, and many Secretaries of States' offices.

NATIONAL ASSOCIATION OF STATE WORKFORCE AGENCIES

The National Association of State Workforce Agencies (NASWA) is a non-profit organization composed of representatives from 54 states and territories' workforce agencies. The organization started in 1937 to help states coordinate with the federal government on the administration of then-new state unemployment compensation laws. They run several shared services for state unemployment insurance programs, and one of those is the Integrity Data Hub.

In 2020, states were faced with unprecedented levels of fraudulent unemployment benefits claims by large-scale organized crime rings. States fought this by teaming up to use NASWA's Integrity Data Hub, an API that states can use to verify new claims against a database of known-fraudulent claims. The Integrity Data Hub combines a suspicious actor repository, a collection of suspicious email domains, interstate claims cross-matching, and data analysis of claims content. NASWA reports that over half-a-billion dollars in fraudulent payments have been caught by the Integrity Data Hub so far. Any single state could perform this sort of scan of claims on their own, but that wouldn't be nearly as effective as all states pooling their data. The cooperative, federated data-sharing model makes the Integrity Data Hub a powerful, important source for identifying bad actors.

NASWA's Integrity Data Hub is not currently a component of Login.gov.

Cooperatives' Use of Login.gov

Software co-ops provide data and services that are valuable for verifying identities, but co-ops could also benefit from Login.gov-provided identity verification services.

The clearest use case is for software co-ops to modify their software to provide built-in support for identity verification via Login.gov. Most software co-ops provide software for which identity is unimportant, but there are notable exceptions.

A significant example is the newly announced effort by the U.S. Department of Labor (DOL) to develop shared software for the collective needs of state unemployment insurance (UI) systems. Identity verification is famously important for the provision of benefits, and DOL baking in support for Login.gov would substantially simplify the adoption process by state labor agencies. There are several existing interstate UI cooperatives, shared by just a few states each, where there would be similar benefits.

There is non-obvious value in cooperatives adding Login.gov support: the creation of a virtuous cycle. States provide identity verification data to co-ops, which share that data with Login.gov, and state agencies can then use cooperative software that verify identities using the state's own data. This cycle builds sustainability and provides incentives for providing timely, accurate data.

More cooperatives are likely to adopt the support for Login.gov insofar as it is non-invasive. If identity verification requires also incorporating Login.gov's account management, that's going to be more difficult. But if Login.gov added standalone identity verification, then adding support could be as simple as adding an API call. Login.gov-provided software development kits (SDK) in the major programming languages could make this a copy-and-paste exercise for cooperatives.

An Ideal Future State for Login.gov

At present, Login.gov is significantly limited in its scope and services, due to policy restrictions and their obligation to be cost-recoverable. What might an ideal state of Login.gov look like?

First and foremost, Login.gov should be extremely inexpensive for agencies to participate in. Free might be too cheap—a thing without cost can be treated as worthless—but the obligation to be cost-recoverable ignores the enormous cost savings that come from having government systems be secure.

Second, Login.gov should be available to all levels of government throughout the United States: state, local, tribal, and territorial.

Third, Login.gov's scope of services should use a more expansive definition of "account services." In addition to account management, it could incorporate services like eligibility determination (using the Federal Data Services Hub) and communications preferences and delivery (using Notify)—the former being an important part of the account creation process for benefits services, the latter being useful for nearly every government service. There are additional straightforward functions that could be part of Login.gov, such as giving people a single location to update their physical address that would carry through to all participating agencies (boards of election, departments of taxation, DMVs, etc.), that become possible when considering a broader role for Login.gov.

Fourth, Login.gov should partner with the U.S. Postal Service to allow in-person identity verification at every post office in the United States. This would sidestep the challenges of online identity verification, allowing people to display a government-issued photo ID over the post office counter and have their identity verified on Login.gov, and for all services that rely on it for IVaaS.

Finally, Login.gov services should be severable, whenever possible, so that participating agencies need not replace their authentication system with Login.gov's in order to benefit from its services.

Conclusion

Interagency software cooperatives are uniquely positioned to facilitate the creation of a federated digital identity verification service that respects the country's federated approach to identity. In the cases of AAMVA and NAPHSIS, they are literally the only way to get their respective data types from states, and each of those data types are foundational to any identity verification system.

A national identity verification system should rely on state data directly from states, to ensure accuracy, timeliness, and confidentiality. It can emulate the existing physical ID authentication model by using existing infrastructure, requiring nothing more than new data-sharing agreements with organizations that are accustomed to such data-sharing agreements. The U.S. can employ the nation's proven, federated identity service as its identity verification system and let government entities focus on carrying out their missions and delivering services to the public.