



Digital Identity Verification

Best Practices for Public Agencies



The **Center for Democracy & Technology (CDT)** is a 27-year-old 501(c)3 nonpartisan nonprofit organization that fights to put democracy and human rights at the center of the digital revolution. It works to promote democratic values by shaping technology policy and architecture, with a focus on equity and justice. The organization is headquartered in Washington, D.C. and has a Europe Office in Brussels, Belgium.

As governments expand their use of technology and data, it is critical that they do so in ways that affirm individual privacy, respect civil rights, foster inclusive participatory systems, promote transparent and accountable oversight, and advance just social structures within the broader community. CDT's **Equity in Civic Technology Project** furthers these goals by providing balanced advocacy that promotes the responsible use of data and technology while protecting the privacy and civil rights of individuals. We engage with these issues from both technical and policy-minded perspectives, creating solutions-oriented policy resources and actionable technical guidance.

Digital Identity Verification

Best Practices for Public Agencies

Authors

Michael Yang
Elizabeth Laird

Footnotes in this report include original links as well as links archived and shortened by the [Perma.cc](#) service. The Perma.cc links also contain information on the date of retrieval and archive.

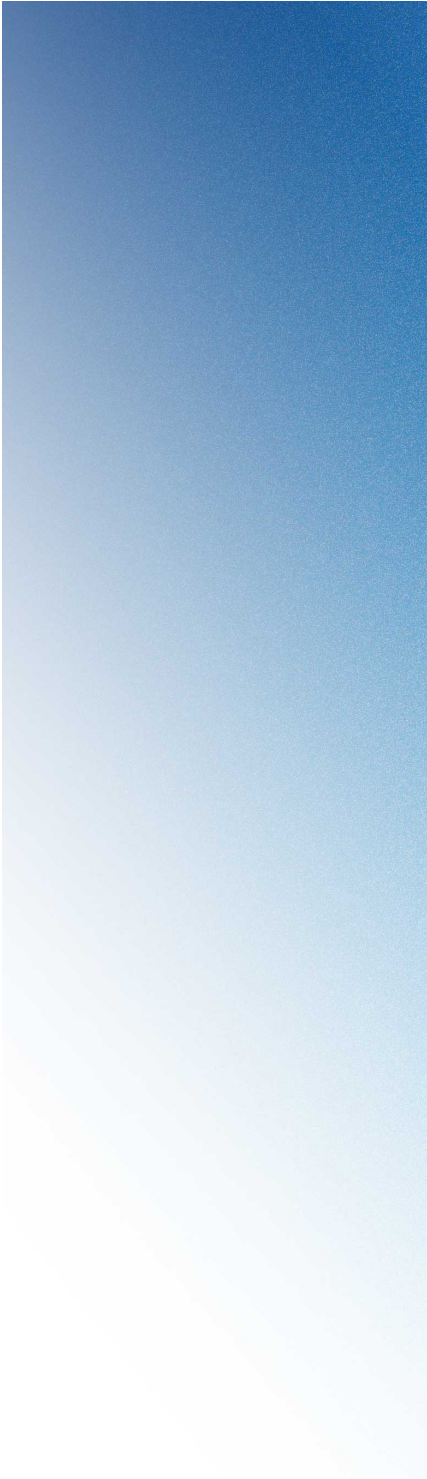
October 2022



Table of Contents

Introduction	5
Benefits of Digital Verification	6
Challenges of Digital Verification	7
<i>Higher Rates of Identity Fraud</i>	<i>7</i>
<i>Equitable Access</i>	<i>8</i>
<i>Highly Sensitive Information</i>	<i>9</i>
<i>Cost Implications</i>	<i>10</i>
Types of Digital Verification Techniques	11
<i>Videoconferencing</i>	<i>11</i>
<i>Matching Government Data with Information Held by Private Vendors</i>	<i>12</i>
<i>Intergovernmental Data Sharing</i>	<i>13</i>
<i>Existing Intergovernmental Data Sharing Efforts</i>	<i>15</i>
<i>Biometrics</i>	<i>17</i>
Best Practices	18
Conclusion	21

Introduction



One of the cornerstones of government service is identity verification, or the process of validating an applicant's claim that they are who they say they are. Traditionally, identity verification has required the physical presence of the individual whose identity needed to be verified.

Digital verification, by contrast, occurs partially or fully over the internet. Digital identity verification offers several potential advantages over traditional verification, but these benefits can only be achieved if issues related to privacy and ethical data use are also addressed. This guidance surveys the challenges facing government agencies who want to digitally verify identities as part of improving service delivery, and provides recommendations about how to address those challenges.

Benefits of Digital Verification

Digital identity verification can have several advantages as compared to traditional identity verification methods.

First, digital verification can be more **accessible**. Applicants no longer have to find time outside of work to travel to a possibly distant office to file for benefits. Physical restrictions may prevent many from applying in person, whether due to public health restrictions or pre-existing health conditions. Digital verification could also reduce redundant information collection by pooling an applicant's existing information across different sources. In a similar vein, digital verification also has the potential to be **faster**, since many more applications can be processed simultaneously compared to manual human review.

Finally, digital verification could ultimately **improve the quality of service** delivered by government agencies. If modernized identity verification can quickly and accurately process a majority of applications, administrators will have more time and resources to deal with other aspects of service delivery, including more complicated cases.

Challenges of Digital Verification

Verifying the identity of applicants who are not physically present pose a tricky problem for government agencies. Identity verification in general challenges government agencies to both deliver services in a timely manner and prevent fraud, goals that are in tension with each other. Agencies can be more risk sensitive and vet applications more thoroughly for fraud, at the cost of time and service quality to the applicant. On the other hand, they can be less risk-sensitive and deliver benefits with less verification, at the cost of increased fraud. COVID-19 pandemic assistance was a prime example of a risk-insensitive approach, where the focus was on delivering benefits as quickly as possible even at the risk of greater fraud.

In addition to these general challenges affecting all types of identity verification, digital verification presents several unique challenges:

- Digital verification has **higher rates of identity fraud** compared to non-digital verification.
- **Providing equitable access** to all users of government services can be difficult.
- Digital verification data is **highly sensitive and presents increased privacy risks**.
- Measures to address these problems can **increase the cost of online services**.

Higher Rates of Identity Fraud

Digital identity verification is **inherently more prone to fraud than in-person services are**. Traditionally, in-person verification is very resistant to identity fraud; it's difficult to imitate even a single identity while physically present, let alone do so en masse. In contrast, digital verification allows bad actors to submit fraudulent applications at scale. When organized criminals discover a new vulnerability in an existing digital verification technology, they can quickly leverage the technological loophole and submit vast numbers of fraudulent applications with the assistance of computers. Because of the speed of computers and the internet, such criminals can cause a great deal of harm before the vulnerabilities can be fixed.

We saw an example of how digital verification can fail at scale during the COVID-19 pandemic. Organized criminals from both the U.S. and abroad exploited a vulnerability

in *knowledge-based checks*, one method for identity verification, to steal as much as \$163 billion from COVID-related unemployment insurance.^{1,2} In a knowledge-based check (KBC), users prove identity by correctly answering online quizzes about pieces of information such as a previous address, their social security number, or the size of their mortgage. The theory behind this identity verification technique is that only legitimate users should know the answers to the questions posed in the KBC, but many KBCs are now insecure due to the availability of personal information online from stolen or hacked data.³ KBCs were known to be insecure as early as 2017, when the Equifax data breach occurred, exposing tremendous amounts of personal data. However, many government agencies at all levels continued to use them – including during the pandemic.^{4,5,6}

Equitable Access

Providing equitable access to all customers of government service, including **those without access to technology** and **members of marginalized groups**, is another challenge for digital verification. First, not all individuals will have access to the technology, such as an internet-connected device or a webcam, to successfully complete digital verification. Roughly a quarter of people in the U.S. don't have broadband internet access at home, and that figure increases for Black and Hispanic households.⁷

Similarly, the biometric techniques used for some kinds of digital verification may also perform less well for marginalized groups. Biometric verification is the use of technology to recognize individuals based on unique physical and biological features. In the context of government services, one of the most used biometric features are facial photographs, but the use of technology to automatically recognize faces may be less accurate across different racial groups.⁸

- 1 Cezary Podkul. [How Unemployment Insurance Fraud Exploded During the Pandemic](https://perma.cc/WKR4-EJAM). ProPublica (July 26, 2021) [<https://perma.cc/WKR4-EJAM>].
- 2 [OIG Oversight of the Unemployment Insurance Plan](https://perma.cc/L5U9-T4MB). U.S. Department of Labor (September 22, 2022) [<https://perma.cc/L5U9-T4MB>].
- 3 J. Carlton Collins. [Check on data breaches at the Privacy Rights Clearinghouse](https://perma.cc/2LT5-FK3A). Journal of Accountancy (September 1, 2019) [<https://perma.cc/2LT5-FK3A>].
- 4 [Data Protection: Federal Agencies Need to Strengthen Online Identity Verification Processes](https://perma.cc/KL5N-72RY). United States Government Accountability Office (May 17, 2019) [<https://perma.cc/KL5N-72RY>].
- 5 [Equifax Data Breach Settlement](https://perma.cc/3W3F-RW25). Federal Trade Commission (February 2022) [<https://perma.cc/3W3F-RW25>].
- 6 Waldo Jaquith. [Software Co-ops and Digital Identity: How U.S. State and Local Governments are Adapting Login.gov to Verify Identity](https://perma.cc/TTU2-9V8C). Beek Center for Social Impact + Innovation at Georgetown University (October 14, 2021) [<https://perma.cc/TTU2-9V8C>].
- 7 [Internet/Broadband Fact Sheet](https://perma.cc/P2HF-YKY9). Pew Research Center (April 7, 2021) [<https://perma.cc/P2HF-YKY9>].
- 8 Nicol Turner Lee. [Mitigating bias and equity in use of facial recognition technology by the U.S. Customs and Border Protection](https://perma.cc/74SL-LJA9). The Brookings Institution (July 27, 2022) [<https://perma.cc/74SL-LJA9>].

Highly Sensitive Information

Protecting user privacy is also a challenge since the data collected during the process of identity verification is highly sensitive. Digital verification schemes need to both **protect user data from attackers using proper security practices** and **guard against harmful secondary uses through rigorous privacy policies**. First, user data may be leaked accidentally or through forced means.^{9,10} As mentioned previously, such data can often be used to subvert identity verification in the future, causing harm both to government agencies, who are stolen from, and to individuals, who become victims of identity theft. Individuals face significant obstacles in regaining access to government services when agencies put a red flag on legitimate identities that were used for fraud.¹¹ Furthermore, the Federal Trade Commission registered 400,000 identity theft complaints in 2020, a 3000% increase from the prior year.¹² The consequences of identity theft on its victims highlights the importance of protecting identity data in the first place.

Second, identity verification data can be used for harmful secondary purposes. Vendors providing digital verification services may resell data to other businesses or back to the government itself.^{13,14} Government-managed databases initially created for benefits may be repurposed for law enforcement.¹⁵ These practices run against the goal of restoring citizens' trust in government services, since a fear of what the government will do with citizens' data may cause individuals to stop engaging with government agencies.¹⁶

-
- 9 Caroline Haskins. [Democrat senators call ID.me's handling of user data 'careless, irresponsible, and improper' after Insider report](https://perma.cc/67GM-QVRZ). Insider (June 8, 2022) [<https://perma.cc/67GM-QVRZ>].
 - 10 J. Carlton Collins. [Check on data breaches at the Privacy Rights Clearinghouse](https://perma.cc/2LT5-FK3A). Journal of Accountancy (September 1, 2019) [<https://perma.cc/2LT5-FK3A>].
 - 11 Cezary Podkul. [How Unemployment Insurance Fraud Exploded During the Pandemic](https://perma.cc/WKR4-EJAM). ProPublica (July 26, 2021) [<https://perma.cc/WKR4-EJAM>].
 - 12 [Consumer Sentinel Network Data Book 2020](https://perma.cc/63T4-BJDF). Federal Trade Commission (February 2021) [<https://perma.cc/63T4-BJDF>].
 - 13 Joseph Cox. [LexisNexis to Pay \\$5 Million Class Action Settlement for Selling DMV Data](https://perma.cc/4CHR-7QEB). Motherboard (November 5, 2020) [<https://perma.cc/4CHR-7QEB>].
 - 14 Elizabeth Goitein. [The government can't seize your digital data. Except by buying it](https://perma.cc/4MXQ-4NSA). The Washington Post (April 26, 2021) [<https://perma.cc/4MXQ-4NSA>].
 - 15 [Deferred Action for Childhood Arrivals \("DACA"\)](https://perma.cc/43ZA-2QSX). Electronic Privacy Information Center [<https://perma.cc/43ZA-2QSX>].
 - 16 Michael Wines. [Critics Say Questions About Citizenship Could Wreck Chances for an Accurate Census](https://perma.cc/2X76-QR9F). The New York Times (January 2, 2018) [<https://perma.cc/2X76-QR9F>].

Cost Implications

Finally, though government agencies may initially deploy online services with the goal of saving costs, inappropriately managed technology can ultimately be **more costly**. First, widespread fraud can inflate the cost of online services. Second, governments have a bad track record with large information technology (IT) projects. 87% of large government software projects fail to meet key objectives on time and within budget.¹⁷ Digital verification, as a kind of IT project, faces similar challenges.

17 Robin Carnahan, Randy Hart, & Waldo Jaquith. [State Software Budgeting Handbook](https://perma.cc/W49N-J54G). 18F (August 2019) [<https://perma.cc/W49N-J54G>].

Types of Digital Verification Techniques

Government agencies have several options for digital verification.¹⁸ An agency may have to use several of the following techniques to securely implement digital verification. These options include:

- Using **videoconferencing** software to digitally replicate in-person verification
- Matching government data with information held by **private vendors** to validate the information presented by an applicant
- **Sharing data** with other government agencies
- Using **biometric** technologies

Videoconferencing

The increase in quality, resolution, and speed of videoconferencing enables “remote supervised” verification.¹⁹ In this approach, the applicant participates in a videoconferencing call with a verifier, who may be a government employee or contractor. To confirm the applicant’s identity, the verifier may ask the applicant a series of questions as well as ask the applicant to present identification documents.

Providing an option for in-person verification via videoconferencing could provide similar fraud-prevention benefits to physical in-person verification while also providing some of

18 At the time of writing, other technologies that may be discussed in the context of identity are not yet ready for widespread usage. These technologies include the use of consumer biometric devices, digital driver’s licenses, and Blockchain.

[FIDO Government Deployments and Recognitions](https://perma.cc/FMX7-WQBQ). FIDO Alliance (February 18, 2022) [<https://perma.cc/FMX7-WQBQ>].

Jay Stanley. [Digital IDs Might Sound Like a Good Idea, But They Could Be a Privacy Nightmare](https://perma.cc/U3SF-2MJL). American Civil Liberties Union (May 17, 2021) [<https://perma.cc/U3SF-2MJL>].

[Blockchain: Emerging Technology Offers Benefits for Some Applications but Faces Challenges](https://perma.cc/A69D-GHMA). Government Accountability office (March 23, 2022) [<https://perma.cc/A69D-GHMA>].

19 [Supervised Remote Identity Proofing](https://perma.cc/B63R-DECY). National Institute of Standards and Technology (July 1, 2020) [<https://perma.cc/B63R-DECY>].

the convenience of digital verification to users. The following guidelines help ensure that a “remote supervised” verification session is as secure as possible:²⁰

- Ensure that the verifier (the individual trained in identity verification) monitors the entire verification session; and
- Require that the user claiming an identity does **not** leave the video frame for the entirety of the session, and that all of the user’s actions are visible in the video frame.

For government agencies with staff already trained in identity verification, offering videoconferencing to complement online services could be relatively simple and obviate the need for procuring vendors. If done correctly, verification through videoconferencing will also be highly fraud-resistant. However, videoconferencing also presents equity issues as it relies on webcam and internet access that not all prospective applicants may have, and it may not provide the same potential cost efficiencies as more automated forms of digital identity verification.

Matching Government Data with Information Held by Private Vendors

A government agency can seek to verify the authenticity of an application by checking – in a variety of sources – that records exist for a several data elements like a user’s claimed name, phone number, and address. This process is called *attribute validation*. Government agencies can accomplish attribute validation either through the procurement of private vendors (the focus of this section) or by sharing data with other governmental entities (see next section).

Private vendors for attribute validation collect, aggregate, and provide access to preexisting user records, such as credit bureaus that maintain financial histories of individuals in order to generate credit reports. For example, private credit agencies are one provider of *knowledge-based checks*, the kind of identity verification that has been both popular and insecure in the past (see above section on challenges of digital verification).²¹

Attribute validation merely confirms that an identity exists, and doesn’t confirm whether the presenting individual can be tied to that identity. Thus, agencies may need to use further methods for identity verification. For example, once a record’s existence has been confirmed, the agency can send a temporary passcode using information that is in the record like a known physical address (more secure), phone number (somewhat secure) or email (less secure) tied to the user.

20 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf>, section 5.3.3.2 [<https://perma.cc/P24W-TCC2>].

21 Jennifer Wagner & Genevieve Gaudet. [Removing Barriers to Access From Remote Identity Proofing](#). Center on Budget and Policy Priorities (April 22, 2020) [<https://perma.cc/9RBB-XCZ6>].

There are drawbacks to this arrangement, however. First, from a cost perspective, government agencies may foot a high bill if they give data to private companies that then sell access to that data back to the government.²² Second, there are significant privacy risks to users. One kind occurs from accidental leaks, but another is deliberate, as private identity companies can also sell access to identity data to other companies, such as health insurance.²³ Such data can be used to track whether a user is a recipient of government services and selectively offer, modify, or deny service to such individuals, as well as other secondary purposes.

Intergovernmental Data Sharing

When users interact with multiple government agencies, they often have to complete identity verification individually for each point of interaction. Sharing of information between government agencies, if done properly, could cut down on redundant data collection and identity verification while also preventing fraud.²⁴ Government agencies can use shared data to verify identities in several ways:

- *Attribute validation:* Governmental agencies can provide similar services as private vendors by allowing other agencies to cross-check user information. For example, the state agencies for SNAP benefits and for Medicaid benefits could provide limited access to their user records for the other to check.
- *Knowledge-based checks:* Like the knowledge-based checks administered by private credit agencies, governmental agencies can help verify identities by asking applicants for information that is private to them and another government agency.²⁵ For example, a state health insurance exchange could create a knowledge-based check asking an applicant to correctly identify which insurance carrier they use. Other agencies can then use this check as part of their identity verification process.
 - » However, as with other forms of knowledge-based checks, government agencies must take care to only use information that is private to them and the user. Any data that has been leaked previously or is already part of the public domain (such as voting records) should not be used for knowledge-based checks. Even with these constraints, knowledge-based checks could still be a valuable form of intergovernmental data sharing, since interactions between users and agencies often generate new pieces of information.

22 Bill Hunt. [What Login.gov's Expansion Means for Local, State & Federal Government](https://perma.cc/U2CC-LXFQ). GovLoop (February 23, 2021) [https://perma.cc/U2CC-LXFQ].

23 Marshall Allen. [Health Insurers Are Vacuuming Up Details About You — And It Could Raise Your Rates](https://perma.cc/359Q-MH3J). ProPublica (July 17, 2018) [https://perma.cc/359Q-MH3J].

24 [Key Practices to Reduce Improper Payments through Identity Verification](https://perma.cc/W8DQ-GX4P). The Joint Financial Management Improvement Program (July 2022) [https://perma.cc/W8DQ-GX4P].

25 Jennifer Wagner & Genevieve Gaudet. [Removing Barriers to Access From Remote Identity Proofing](https://perma.cc/9RBB-XCZ6). Center on Budget and Policy Priorities (April 22, 2020) [https://perma.cc/9RBB-XCZ6].

- *Sharing known cases of fraud:* Governmental agencies should coordinate to handle known or suspected cases of fraud. This might be as simple as sharing user records that have been known to be part of fraud attempts. More complicated efforts involve sharing technical indicators like IP addresses of known fraudsters.²⁶

Sharing data between government agencies is not free of downsides. Two important issues are privacy and cost. First, unchecked sharing and storage of data within government can result in harmful secondary uses. For example, a database originally meant to enable child immigrants to obtain work permits was later repurposed for deportation.²⁷ Great care must be taken to ensure that data sharing between government agencies is only for the purposes of providing government services, to minimize the data shared, and to limit access to the data.

Second, intergovernmental data sharing may incur costs from meeting legal, technical, and policy requirements. Government agencies may lack the technical infrastructure to share data with other agencies, especially in a manner consistent with privacy law.^{28,29} To remedy this, they may have to invest in personnel, training, and technology in order to modernize their information technology systems.³⁰

26 Hannah Quay-de la Vallee. [Combatting Identify Fraud in Government Benefits Programs: Government Agencies Tackling Identity Fraud Should Look to Cybersecurity Methods, Avoid AI-Driven Approaches that Can Penalize Real Applicants](https://perma.cc/F2LA-A2RM). Center for Democracy and Technology (January 7, 2022) [<https://perma.cc/F2LA-A2RM>].

27 [Deferred Action for Childhood Arrivals \("DACA"\)](https://perma.cc/43ZA-2Q5X). Electronic Privacy Information Center [<https://perma.cc/43ZA-2Q5X>].

28 Kevin H. Wilson. [Sharing Securely within Government: Best Practices for Facilitating Interagency Data Science](https://perma.cc/MUJ2-UMAF). The Lab @ DC (September, 2017) [<https://perma.cc/MUJ2-UMAF>].

29 [Guidance on Inter-Agency Sharing of Personal Data: Protecting Personal Privacy](https://perma.cc/JBG2-M5ZC). The White House (December 20, 2000) [<https://perma.cc/JBG2-M5ZC>].

30 [Provide Funding for State Governments to Modernize Legacy IT Systems](https://perma.cc/QZM4-UXLA). National Association of State Chief Information Officers (January 2021) [<https://perma.cc/QZM4-UXLA>].

Existing Intergovernmental Data Sharing Efforts

Some government agencies have already created technical systems for sharing data that could be useful for digital verification of identities. Two examples of this important work are *data hubs* and the Login.gov *single sign-on for government*.

Data hubs are cooperatives between many government agencies that provide streamlined access to some kinds of data, such as driver's licenses.

Single sign-on is a software protocol for allowing a user to authenticate with many different websites with just one set of credentials. The primary example of single sign-on for U.S. government agencies is [Login.gov](https://login.gov).

Data Hubs

There are three important intergovernmental cooperatives for data sharing, each of which provide records of important identity information:³¹

1. The American Association of Motor Vehicle Administrators (AAMVA) provides access to drivers' license data. Drivers' licenses are important in digital verification because they are a primary identity document (meaning that they are difficult to obtain and forge), and because they provide photographs for biometric verification.
2. The National Association for Public Health Statistics and Information Systems (NAPHSIS) provides access to birth and death records. Birth records help establish that an individual exists, while death records can help prevent fraud by identifying deceptive applications that attempt to use a deceased person's identity.
3. The National Association of State Workforce Agencies (NASWA) shares information on fraudulent unemployment applications, which can help other agencies coordinate efforts on known or suspected cases of fraud.

All three of these cooperatives provide access to their data via APIs, meaning that software developers at other agencies can integrate these data sources into their identity verification software.

31 Waldo Jaquith. [Software Co-ops and Digital Identity: How U.S. State and Local Governments are Adapting Login.gov to Verify Identity](https://perma.cc/TTU2-9V8C). Beeck Center for Social Impact + Innovation at Georgetown University (October 14, 2021) [<https://perma.cc/TTU2-9V8C>].

Governmental Single Sign-On: Login.gov

Login.gov provides users a single account and interface for accessing those government services that have chosen to implement the platform. Login.gov provides a bundle of user account creation and management services, including identity verification. Government agencies can choose to forgo their own bespoke user account services, integrate with Login.gov, and gain access to identity verification through Login.gov. Going this route reduces both the number of accounts a user has to remember and redundant verification checks, since Login.gov can store the result of previous verification checks.

Biometrics

Biometrics are personal information generated from processing unique biological, physical, or physiological characteristics, such as a fingerprint, facial structure, or voice print, and they can play a role in identity verification. For example, public agencies are increasingly deploying facial recognition for identity verification.³² With verification facilitated by facial recognition, a user-submitted selfie photo is compared against a digital scan of the relevant identity document. Though human review is possible, the largest gains in efficiency use automated, computational techniques to automatically extract and compare facial features. Like many other IT products, governmental bodies generally rely on third-party vendors for biometric verification.

In the best-case scenario, facial recognition technology can be fast and convenient for both users and agencies while also being highly fraud-resistant. However, facial recognition also raises equity and privacy risks. In terms of equity, (i) not all individuals have access to an internet-connected device with an adequate camera; and (ii) facial recognition may not perform equally well across different demographic groups.^{33,34}

The use of facial recognition and other biometric data raises significant privacy issues, too, which are further exacerbated by reliance on third-party vendors. Biometric data initially collected to complete identity verification may later be used for surveillance or law enforcement. Secondary use of biometric data is particularly problematic, because biometric data cannot be anonymized or divorced from the user. The possibility for secondary uses also raises the question of vendor security. Vendors may not handle confidential user data securely and safely. Unlike, for example, the identity number on a driver's license, biometric information cannot be modified if malicious actors are able to mimic or impersonate said biometrics.

Some of these challenges, such as vendor privacy concerns, might be partially ameliorated with better data management practices, like limitations on vendor data retention and audits of vendor practices. Other issues, like equitable access or misidentification, are unlikely to be addressed in the short term. Further recommendations about using biometrics for identity verification can be found in previous CDT guidance.³⁵

32 Shawn Donnan and Dina Bass. [How Did ID.me Get Between You and Your Identity?](https://perma.cc/MTD4-YW28). Bloomberg (January 20, 2022) [<https://perma.cc/MTD4-YW28>].

33 Natalie Alms. [No easy fix for ID verification for government benefits](https://perma.cc/KH78-DP3L). FCW (January 24, 2022) [<https://perma.cc/KH78-DP3L>].

34 Nicol Turner Lee. [Mitigating bias and equity in use of facial recognition technology by the U.S. Customs and Border Protection](https://perma.cc/74SL-LJA9). The Brookings Institution (July 27, 2022) [<https://perma.cc/74SL-LJA9>].

35 Hannah Quay-de la Vallee. [Public Agencies' Use of Biometrics to Prevent Fraud and Abuse: Risks and Alternatives](https://perma.cc/9ZE4-RY5P). Center for Democracy and Technology (June 7, 2022) [<https://perma.cc/9ZE4-RY5P>].

Best Practices

As public agencies move to improve service delivery through digitally verifying identities, they should adhere to the following best practices in order to minimize fraud, avoid discrimination and inequitable access, and protect citizens' privacy:

- **Minimize fraud with techniques from cybersecurity:**³⁶ A key challenge for digital verification is preventing identity fraud. Public agencies can address this risk, in part, by using cybersecurity techniques to make digital verification more fraud-resistant. Coordinated attacks from organized criminals might be uncovered by a variety of technical indicators, such as IP addresses from foreign countries or application forms filled out in an unreasonably short amount of time. Additional barriers, such as CAPTCHA challenges or two-factor authentication via previously known phone numbers, or emails can also deter criminals while being relatively easy to surmount for legitimate users. Even if none of the cybersecurity measures themselves can positively validate a user's identity, they can be helpful in screening out clearly fraudulent applications.
- **Provide non-digital alternatives:** Non-digital alternatives can be helpful for both preventing fraud and providing equitable access. Situations in which a user needs a non-digital alternative include: when a legitimate user cannot successfully pass automated screens like facial recognition or attribute validation; when a legitimate user files an application that has already been the target of an identity theft attempt; and when a user lacks internet access to complete digital verification. Possible non-digital alternatives include verification via a one-time code sent through postal mail and in-person verification at local offices.
- **Implement privacy-forward data governance policies and practices:** Given the particularly sensitive nature of identity attributes and biometric information, public agencies should enact privacy policies and practices that ensure safe collection and storage of user data, including:

36 Hannah Quay-de la Vallee. [Combating Identify Fraud in Government Benefits Programs: Government Agencies Tackling Identity Fraud Should Look to Cybersecurity Methods, Avoid AI-Driven Approaches that Can Penalize Real Applicants](https://perma.cc/F2LA-A2RM). Center for Democracy and Technology (January 7, 2022) [<https://perma.cc/F2LA-A2RM>].

- » **Take a data minimization approach to collecting and storing data.** Government agencies should collect, process, and retain only the data that is required to provide the given services. They should delete that data once it is no longer needed. Data that is no longer useful creates an unnecessary privacy risk to users, as that data can then be erroneously accessed or breached.
- » **Additionally, take a data minimization approach to sharing data.** When working with others, government agencies should share only as much data with other agencies and vendors as is needed to assist with identity verification. Instead of requesting full user records, agencies can instead choose to request the agency hosting the data to simply answer, “Do you have this set of records in your database?” Doing so minimizes the transfer of user data across agencies.
- » **Limit secondary uses of data.** Agencies can do so either by adopting formal policies that prohibit secondary uses by themselves or any party with which data is shared, or by requiring affirmative, informed consent for each specific secondary use. In all events, agencies should explicitly prohibit uses that pose the risk of harm to users, such as law enforcement or immigration enforcement uses.
- » **Limit internal access to data to only those who need access to perform their job duties.** Restricting internal access serves both to protect the privacy of users from unneeded viewing and to limit the potential for data breaches.³⁷ Furthermore, data access should only be granted on a time-limited basis.
- **Plan and test systems with equity in mind.** Public agencies should develop plans to test their identity verification systems on diverse populations across protected categories like race, gender identity, and disability.³⁸ This testing is all the more important in the context of government service delivery, since those who need access to those services are likely to fall into one or more of those groups.³⁹
- **Develop clear standards, requirements, and processes for procuring and auditing third-party systems used in identity verification.**
 - » Agencies should ensure that the requirements for third-party systems are met by establishing a clear and stringent procurement process. The process should include gathering and evaluating information about how the vendor meets the

37 Elizabeth Laird & Hannah Quay-de la Vallee. [Data Sharing & Privacy Demands in Education: How to Protect Students While Satisfying Policy & Legal Requirements](#). Center for Democracy and Technology (November 13, 2019) [<https://perma.cc/2JLQ-DP6W>].

38 Henry Claypool, Claire Carey, Alexander C. Hart, & Linnea Lassiter. [Centering Disability in Technology Policy: Issue Landscape and Potential Opportunities for Action](#). American Association of People with Disabilities & the Center for Democracy and Technology (December 13, 2021) [<https://perma.cc/5QWA-KF2F>].

39 Rich Morin, Paul Taylor, & Eileen Patten. [A Bipartisan Nation of Beneficiaries](#). Pew Research Center (December 18, 2012) [<https://perma.cc/YSE7-GV2P>].

same standards to which government agencies are held, for both secure and private handling of data and equitable performance across protected groups.

- » Agencies should hire for the necessary internal expertise or allocate the necessary auditing resources to review the documentation provided by potential vendors to ensure that their practices are sufficient, and request additional documentation as needed. This will mean both technical expertise to ensure the system will function as expected and legal expertise to ensure that the system (and its intended use) conforms to any applicable laws.
- » The review process should be repeated periodically for as long as the vendor system is in use, to ensure that the system continues to comply in the face of updates to the system or internal policies.
- » Because identity verification is a common problem for many agencies, agencies should share their knowledge and experience with different vendors. A good starting point is the U.S. Digital Response's review of identity vendors.⁴⁰

40 [Unemployment Insurance Modernization: Summary of vendor offerings](https://perma.cc/PN65-QYUE). United States Digital Response (October 13, 2021) [<https://perma.cc/PN65-QYUE>].

Conclusion





Digital verification of identity can help government agencies provide services more quickly and conveniently.

For digital verification to deliver on those promises, government agencies must take care to minimize fraud, avoid discrimination and inequitable outcomes, and protect privacy. Our set of recommendations can help government agencies do so and improve user trust in quality government services.

 cdt.org

 cdt.org/contact

 Center for Democracy & Technology
1401 K Street NW, Suite 200
Washington, D.C. 20005

 202-637-9800

 @CenDemTech