

Public Agencies' Use of Biometrics to Prevent Fraud and Abuse: Risks and Alternatives

One unexpected consequence of the COVID pandemic has been to accelerate public agencies' reliance on biometric technology to verify identities. The pandemic increased the number of people seeking and qualifying for benefits and led to an [expansion of benefits available](#) in order to offer assistance to those struggling with the wave of job loss and other economic and social difficulties. These expanded benefits also led to a [significant increase in attempted fraud](#), both of traditional individual fraudulent actors and of organized crime and nation-state actors engaging in large-scale fraud. The issue of fraud in pandemic-related benefits even drew the attention of the Biden administration, which released [a fact sheet](#) on steps to combat fraud and identity theft in connection with pandemic relief programs. Additionally, the increase in benefits led to challenges in delivering services in an efficient way, as existing systems were not designed for the volume of applicants. This led to long wait times for individuals looking to receive benefits.

To address these dual issues of fraud and inefficiency (or waste), many agencies turned to biometric-based systems, both to help more effectively identify fraudulent actors to avoid paying out erroneous benefits or avoid providing services to ineligible individuals and more quickly verify legitimate applicants to distribute benefits in an efficient way. As technology is allowing more digital interactions between people and the government, the question of identity verification has become more complex, as agencies can no longer rely on in-person verification with a government ID, nor is it always feasible for beneficiaries. As a result, public agencies are increasingly turning to data sharing and technology to make service delivery easier and more efficient while limiting fraud and waste.

Public agencies' efforts to use biometrics technology to prevent fraud and waste raises a number of concerns. This guidance sets forth best practices for government agencies, both in assessing whether alternatives are available and how to mitigate some of the privacy and equity risks associated with reliance on biometric data.



Overview of the Use of Biometrics for Identity Verification

Biometrics are personal information generated from processing unique biological, physical, or physiological characteristics, such as a fingerprint, facial structure, or voice print. Biometrics-based systems have two key benefits in preventing fraud and waste in a public benefits context. First, if implemented correctly, they can be very easy to use as users do not need to remember a password or keep track of something like a key card or fob. Second, biometric systems can be difficult to trick, though this depends significantly on the particulars of a specific system (for instance, a poorly-implemented facial recognition system can be circumvented with a high resolution photograph).

Because of these potential benefits, biometric-based systems have been used with the goal of delivering services and preventing fraud and waste in a number of ways:

- **Verify identities:** Systems that aim to verify a user to allow them to claim benefits like [unemployment insurance](#) have been [adopted in at least 20 states](#). These often work by comparing a selfie uploaded by the applicant in real time to existing government documentation like a driver's license.
- **Assign universal identifiers:** Systems like India's [Aadhaar program](#), or South Africa's forthcoming [National Identity System](#), aim to provide a universal identifier linked to a biometric like a fingerprint to verify citizens when they make use of government services, both to ease access to services and to ensure that only the authorized user receives benefits.
- **Verify electronic visits:** Facial recognition or [biometric voice authentication](#) can be used to ensure that an approved care worker is providing services to an approved recipient by requiring the carer or the recipient to engage with the voice or facial recognition system at the time and location of service delivery.

Ultimately, the goal of each of these approaches is to offer benefits to users without significant drain on government resources or causing undue burden to applicants.



Concerns of Biometrics-Based Systems

While biometric systems can provide some benefits and functionality, **they also raise important concerns with respect to privacy and equity:**

- **Data sensitivity:** From a privacy standpoint, biometric data is incredibly sensitive, and its use in government systems typically requires large-scale collection of this information. In particular, two risks stem from the collection and storage of biometric data:
 - **Secondary uses:** Repurposing of sensitive data is always a concern, as it complicates whether the user has consented to the use and can disincentivize users from engaging with government agencies, particularly where the secondary use might be for law enforcement purposes. Secondary use of biometric data is particularly sensitive because it cannot be anonymized or divorced from its subject.
 - **Data breaches:** Unauthorized access to biometric data can be exceptionally harmful because, unlike passwords, people cannot update or change their biometrics.
- **Reliance on private vendors:** Biometric systems are often developed and provided by third-party vendors, which can exacerbate the privacy concerns:
 - **Private company control of user information:** These vendors will have access to both sensitive biometric info and potentially other data, depending on how their systems are designed. Requiring people to give sensitive data to a third party in order to obtain government benefits to which they are entitled presents concerns about the privacy of

their data, who will have access to it, and how it will be used over time. Public agencies can endeavor to limit some of these concerns by contractually maintaining control of user data and restricting how vendors may use it, but this is challenging to do – it requires the vendor to implement robust data management technologies in order to ensure that user data is sufficiently partitioned off in their system, and it requires the agency to have sufficient auditing access on a recurring basis to verify those controls to ensure they are effective.

- **Centralization of information:** Biometric-based systems are complicated to develop. Additionally, they often require contracts with public agencies that issue identity documents like motor vehicle departments, and these contracts can be complex to establish. This means that there are a small number of vendors providing services to multiple agencies (for instance, the third party vendor ID.me contracts with [at least 20 states](#) and was set to verify users logging into the IRS website before being pulled [due to public backlash](#)). Consequently, these vendors may have access to substantial cross-agency data (for instance, the vendor may know the entire set of services accessed by a single individual, even if those services are provided by multiple distinct agencies). Also, if a vendor or agency has other information associated with a single identity, like IP addresses, that information could be used to match users across systems, thus serving as a directory of sorts that could be repurposed for other uses, like law enforcement surveillance.
- **Inequitable access and use:** Use of biometric data also raises equity concerns, given that biometric technology is not universally available, and that some biometric attributes like facial structure or eye movement can be proxies for things like race or disability status. Particular equity concerns include:
 - **Efficacy across disparate populations:** Biometric-based systems do not perform equally well for different populations of users, placing a disproportionate burden on certain communities. For instance, voice recognition systems for electronic visit verification may [pose a challenge for non-verbal users](#), and facial recognition systems have [higher failure rates for people with darker skin tones](#).
 - **Uneven technology access:** Biometric-based systems may also assume a certain level of technology access. For example, facial recognition systems that match against a selfie or live video may not work for those who do not have access to sufficiently advanced smartphones or camera technology.



Alternatives to Using Biometrics to Prevent Fraud and Waste

As described above, biometric-based systems come with inherent privacy and equity issues, so they should only be used when there is no viable alternative (considering both efficacy and cost) that presents a lower level of risk. Before collecting biometrics information in the name of preventing fraud

and waste, public agencies should first consider privacy-forward, less-invasive, and potentially less expensive alternatives like:

- **Investing in robust cybersecurity practices:** A [cybersecurity approach](#), which treats fraud as a systemic and organized issue, can provide agencies with significant mitigation of large-scale or systematic fraud while substantially limiting or avoiding the collection of sensitive and irrevocable biometric data. As part of this, agencies should track and analyze technical indicators of fraud. There are a number such indicators that can help to stymie attackers without unduly impacting legitimate applicants. For example:
 - ***IP addresses linked to a different country*** could indicate an attack by a foreign actor (although agencies should provide technical assistance to users, for example to help users employing a VPN to avoid getting improperly flagged).
 - ***Multiple applications from the same IP address***, physical address, phone number, or device may indicate an organized attack (although agencies should have procedures in place to handle legitimate instances of shared resources like group homes, libraries, or families sharing IP addresses or phone numbers).
 - ***Multiple applications with the same credentials*** (such as a Social Security Number or bank account number) may also indicate an organized attack (although, again, it is important to allow for circumstances like family members sharing a bank account).
 - ***Application forms filled out abnormally quickly*** can indicate a bot, which could be a likely indicator of an attack.

As with all cybersecurity interventions, it is important to consider the totality of the situation when assessing an application, since each individual indicator may be explicable on its own, but reviewing a range or combination of factors can allow agencies to detect likely instances of fraud and respond in an efficient way.

- **Using alternatives to verify identities:** For identity verification, agencies should consider using email, text, or mail message verification for applicants, such as emailing a code to a previously-known email address, perhaps one previously on file with another public agency like a motor vehicle department, and asking the user to verify the code. Additionally, agencies may consider using human-based remote verification of identities, using video conferences to compare faces against an identity document. Although this human-based approach is generally the fall-back used when a biometrics-based facial recognition system does not work, it must be well-resourced to provide an effective form of access. Under-resourced systems have generated [significant delays and challenges](#) for those trying to get verified and access benefits, which can be unsustainable for providing critical benefits.
- **Considering alternative digital identity approaches:** There are other digital approaches to identity verification that may make sense for public agencies depending on the context. For situations where there are likely to be repeated interactions between the user and the agency, approaches like smart cards or fobs distributed to the user via a trusted method that can then be used as proof of identity may be useful tools (though distributing the fobs may introduce

challenges if the user cannot pick one up in person and does not have a reliable mailing address). Additionally, identity provisioning standards based on [public key cryptography](#) (which allows systems to trade information securely and be confident about who is sending the information) such as those developed by the FIDO Alliance still depend on biometrics, but do not require the same frequent transfer of data as real-time image-based human verification.



Best Practices in Using Biometrics to Prevent Fraud and Waste

For public agencies that determine that the above approaches will not be effective in their case, and that biometrics are the best approach, they should adhere to several best practices in order to protect their users:

- **Offer alternative mechanisms for access:** Agencies should offer alternative verification options should a user decide they are not willing to engage in the biometric system, due to its risks or should the biometric system fail. These alternative access mechanisms should not place undue burden on users or be disproportionately difficult for historically marginalized people to access.
- **Ensure equitable outcomes across disparate populations:** The systems that agencies adopt should perform equitably, meaning they do not exhibit different behaviors or success rates, across disparate populations so as to create disproportionately worse outcomes for marginalized people. In doing so, public agencies should take special care to ensure that the systems are effective and accessible to historically marginalized populations. Specifically, public agencies should establish that systems are:
 - Accessible to users with disabilities, particularly if the agency provides disability-related services, or services that are likely to be used by disabled users.
 - Able to adapt to physical changes as users age, particularly if they will be used by children (such as school lunch access).
 - Perform equitably for people across different genders, skin tones, and other personal characteristics.

In order to ensure the systems adhere to these requirements, agencies should take a number of steps. Any data sets used to train or test a biometric system should be reviewed to ensure that they reflect the population of users who will be interacting with the system. For instance, a facial recognition system should be trained and tested on users with a range of skin tones, face shapes, morphologies, and disabilities. Additionally, biometrics systems should be tested on potential users from across the spectrum of the user population to ensure that there are no disparate outcomes that would result in inequitable results, like certain populations experiencing delays in accessing services. In addition to pre-deployment testing, systems should also be [regularly audited](#) to ensure that they continue to perform as expected and remain equitable even after changes like updates to the systems or shifts in the demographics of the user population.

- **Protect the privacy of system users:** Given the particularly sensitive nature of biometric information, public agencies should enact privacy policies and practices that ensure safe collection and storage of biometric information, including:
 - **Store encrypted** or transformed versions of biometric information rather than raw biometric information. For instance, instead of storing a raw image of a user's face, an agency can store a face map, which is essentially a diagram of the position and measurements of the user's facial features that can be matched against features of an image like a selfie.
 - **Limit secondary uses** of biometric data, by adopting formal policies that either prohibit the use of biometric data beyond what's necessary to provide the benefits or services that the user seeks or that require affirmative, informed consent for each specific secondary use. Any secondary use should offer a tangible benefit to users. 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 biometric 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.
 - **Take a data minimization approach** to biometric information, by collecting and processing only the biometric data that is required to provide the given services and deleting 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.
- **Maintain direct control of information collected by third parties:** For vendor-provided systems, there are additional best practices to consider:
 - **Limit data sharing** with the vendor to only the data they need to perform the services they are providing to the agency.
 - **Require that third parties limit access** to this sensitive information.
 - As with agency employees, companies should limit employee access to an as-needed basis.
 - For vendors that offer services to multiple agencies, each agency should be restricted to accessing only its own data. That is, if a user interacts with a state's unemployment agency but not with the state's Medicaid agency, the Medicaid agency should not have access to that user's data, even if both agencies use the same vendor.
 - **Prohibit redisclosure or secondary use** of biometrics information, both within the company as well as externally. Vendors should not be able to share data with other companies or with other divisions within the organization unless it is necessary to provide the services. Users' biometric data should not be repurposed for any other uses such as marketing, training algorithms, or building user profiles.

- **Regularly delete data** based on how long it is needed to deliver services. As with agencies themselves, companies should delete data once it is no longer useful. Additionally, agencies should be able to request verification that data has been deleted, including information like when and how the data was deleted, and who can attest that the data was erased.
- **Develop clear standards, requirements, and processes for procuring and auditing third-party systems:** 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 information about a vendor's privacy and security practices to ensure they meet the standards listed above, and information about how the vendor tests for and ensures equitable performance by their system. Agencies will need internal expertise 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.
- **Foster meaningful community engagement and transparency:** Agencies must provide public fora and/or other channels to explain the systems they are considering or planning to adopt, and to gather public input about the potential ramifications of those systems. Explanations should be provided in multiple forms for varying levels of technical expertise. Agencies should also provide multiple methods for the public to give input – including collection of written comments, and public hearings that allow for in-person and remote online and phone participation – to minimize barriers for affected groups whose perspectives will be instrumental in selecting systems that have more equitable and privacy-protective outcomes.

Public agencies are trying to offer benefits to people quickly and efficiently without paying out fraudulent benefits or claims. **In their effort to do so, agencies are turning to biometric-based systems, but these approaches come with significant risks. The concerns raised by biometric data are difficult to mitigate, and agencies should seriously consider alternative approaches and use biometrics only when there are no viable alternatives.** Should an agency determine biometrics are the best option and the benefits outweigh the considerable risk, they should adhere to user-protective best practices for any system they implement to achieve their goals of assisting individuals while respecting their rights and protecting their dignity.



Resources

- Bias in facial recognition and biometrics -
 - <https://www.nature.com/articles/d41586-020-03186-4>
 - <https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf>

- <https://cdt.org/insights/recognizing-the-threats-congress-must-impose-a-moratorium-on-law-enforcement-use-of-facial-recognition-tech/>
- Service denial caused by biometrics -
 - <https://cdt.org/insights/report-challenging-the-use-of-algorithm-driven-decision-making-in-benefits-determinations-affecting-people-with-disabilities/>
 - <https://www.theguardian.com/society/2019/oct/14/computer-says-no-the-people-trapped-in-universal-credits-black-hole>
 - https://datasociety.net/wp-content/uploads/2021/11/EVV_REPORT_11162021.pdf
- Cybersecurity for fraud detection -
 - <https://www.cisa.gov/uscert/ncas/alerts/aa22-011a>
 - <https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify>
 - <https://cdt.org/insights/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-applicant/>
- Biometrics for service delivery -
 - <https://teamcore.seas.harvard.edu/ai-social-work>
 - <https://cais.usc.edu/news/future-is-bright-for-ai-and-social-work>
 - <https://www.smithsonianmag.com/science-nature/myth-fingerprints-180971640/>
 - <https://sites.rutgers.edu/fingerprinting/no-two-finger-prints-are-alike/>
 - <https://www.m2sys.com/blog/public-safety/ensuring-fair-efficient-service-delivery-biometrics-government/>
 - <https://www.pewtrusts.org/en/research-and-analysis/reports/2020/11/health-care-can-learn-from-global-use-of-biometrics>

This is one in a series of information sheets designed by CDT's Equity in Civic Technology team to give practitioners inside public agencies clear, actionable guidance on how to most responsibly use technology in support of the communities they serve. More info: <https://cdt.org/civic-tech-inventory>.