Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
Comments to the White House Office of Science and Technology Policy (OSTP)

RFI on Public and Private Sector Uses of Biometric Technologies

January 2022
The Better Identity Coalition appreciates the opportunity to provide comments to the White House Office of Science and Technology Policy (OSTP) on its Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies.

As background, the Better Identity Coalition is an organization focused on developing and advancing consensus-driven, cross-sector policy solutions that promote the development and adoption of better solutions for identity verification and authentication. Our members – 27 companies in total – are recognized leaders from different sectors of the economy, encompassing firms in financial services, health care, telecommunications, technology, fintech, payments, and security.

Of note, the Coalition does not exist to advocate for the interests of vendors in the space, though about half of our members are vendors. Rather, our policy priorities are driven by firms that depend on digital identity solutions to run their businesses. Our members are united in their view that government is essential to the development and adoption of better identity and authentication solutions. First, because government policies can catalyze or inhibit innovation in digital identity. And second, because government – as the only authoritative issuer of identity in the United States – has an inherent role to play in the digital identity ecosystem.

The coalition was launched in February 2018 as an initiative of the Center for Cybersecurity Policy & Law, a non-profit dedicated to promoting education and collaboration with policymakers on policies related to cybersecurity. More on the Coalition is available at https://www.betteridentity.org/.

In July of 2018, we published Better Identity in America: A Blueprint for Policymakers⁴ – a document that outlined a comprehensive action plan for the U.S. government to take to improve the state of digital identity in the U.S.

At the core of our Policy Blueprint is the recognition that criminals and other adversaries have caught up with the systems America has used for remote identity proofing and verification, and that the security, privacy, and user experience challenges that this fact presents requires the use of newer and better technologies. Our Blueprint highlights why government – as the only authoritative issuer of identity – is in the single best position to address the challenges we have today and make identity better.

While biometrics are not specifically addressed in our Policy Blueprint, biometrics and other artificial intelligence (AI) enabled technologies are playing an increasing role in remote identity proofing and verification, as well as authentication. Understanding that this RFI is part of a broader OSTP effort to craft an “AI Bill of Rights” and consider what policies should apply to the use of AI, we think it is logical to look at biometrics as one of a number of AI-enabled technologies used in identity and authentication.

As we detail in our response, in many cases, these technologies are delivering great benefits – helping not only to deliver enhanced security and convenience, but also more equitable outcomes.

That said, “many” is not “all,” and there are some legitimate concerns around inappropriate uses of AI in identity, as well as questions as to the appropriate boundaries around where and how these technologies should be used. On balance, we believe the benefits exceed the harms today, but harms – both actual and potential – certainly exist. It is critical that any policy efforts are crafted in a way that maximizes potential benefits from AI in the use of identity solutions while minimizing the harms.

We have arranged our response in two sections: one that outlines our general policy recommendations, and a second that is a more in-depth discussion on how AI is being used in identity verification and authentication today. The latter addresses RFI Topics 1 and 5, while the policy recommendations address Topics 1, 2, 5, and 6.

I. Policy Recommendations

As OSTP considers the appropriate use of biometric technologies and other AI-enabled tools in identity verification and authentication, we offer eight key points:

1. AI technologies are an increasingly important tool in identity – particularly given the ongoing battle we are in against cybercriminals. These criminals are doubling or in some cases quintupling down on identity-centric attacks, putting the security and privacy of people’s data and money at risk. The good guys need every tool in the toolbox to guard against these attacks.

   AI-enabled identity tools are emerging in the market, in part, to address some of the key challenges that NIST flagged in its Digital Identity Guidelines, when it stated:

   “Digital identity presents a technical challenge because this process often involves proofing individuals over an open network, and always involves the authentication of individual subjects over an open network. The processes and technologies to establish and use digital identities offer multiple opportunities for impersonation and other attacks."  

   On that point, criminals themselves are starting to develop their own AI-powered tools to support cyber-attacks. While terrifying, this should not be surprising; the same technology innovations that can be used to protect us will also be exploited by adversaries to try to attack us. Our members are seeing this in the early stages with criminals and nation-states using AI-powered bots to launch automated password spray and credential stuffing attacks. Attackers are always innovating, and we should be preparing for them to be using AI against us in new and innovative ways.

2. To the point that there are policy concerns about the use of AI, the answer is not to ban its use but rather to identify the specific concerns and craft policies to address them. A

---

blanket ban on certain technologies will almost certainly play into the hands of criminals and put consumers and businesses at great risk. Likewise, restrictions that are not narrowly tailored to address specific risks or harms may inadvertently preclude constructive applications of AI-powered identity tools. Finally, to the extent existing laws and policies on privacy, security, and human rights already regulate AI, any new AI policy or “AI Bill of Rights” should not contradict or duplicate this, but rather build upon existing legislation.

3. It is important that policymakers do not lose sight of the ways AI and ML can help with inclusion and equity. Financial services firms are already starting to use AI to enable new approaches to identity proofing that can help bring more services to the “credit invisible” – such as more easily auto-approving more people for loans – relative to legacy tools that don’t use AI.

While there are some concerns that algorithms used here might be biased – and that “putting the machines in charge” will lead to inequitable outcomes – most of what we have seen in the use of AI in these types of solutions is improving equity and inclusion. For example, if a bank is looking at credit report data for identity proofing, but a consumer has a thin file (as is common for young people, immigrants, and historically marginalized groups), some AI-enabled tools can be used to incorporate and analyze alternative data sources and approve applicants at a higher rate. Tools that leverage AI are often able to help fill in the “gaps” and provide an alternative path to approval. Likewise, if someone with a thin file has a driver’s license, AI-enabled tools that validate whether an ID document is real or counterfeit – and use biometrics to analyze whether the selfie matches the photo on the ID – can be used to enable easy digital account opening.

4. An important part of issues surrounding the use of AI in identity verification is the fact that many of the technologies are opaque: despite the efficiency of many algorithms, it still difficult to explain their decisions to most people. Moreover, performance of what at first glance looks to be similar products may vary, with some products delivering results that are accurate and equitable, while others do not. We have seen a number of instances where unreliable products fail and then the entire industry is faced with allegations of “bias” – when the issue is not the industry but certain vendors, or how their technology is applied.

These issues can be greatly mitigated by independent certification and testing programs that can evaluate vendor claims and validate what works, what does not, and how.

There is good work underway here today in the identity sector: FIDO Alliance (an identity standards and certification body with both industry and government participation) has launched an initiative to create a new testing and certification program for remote ID proofing tools – creating a way to independently validate the
claims made by vendors and also determine whether there are any specific quirks or biases in a product or algorithm that may need to be addressed.\(^3\) In addition, NIST has done some great work to help vendors and implementers address potential bias concerns in its recent draft Special Publication 1270, “A Proposal for Identifying and Managing Bias in Artificial Intelligence.”\(^4\)

The Treasury Department’s Financial Crimes Enforcement Network (FinCEN) and the Federal Deposit Insurance Corporation (FDIC) have also engaged on this front – on January 11, they announced a new Tech Sprint effort focused on measuring the effectiveness of digital identity proofing for financial services. In their announcement\(^5\) they noted:

> “Digital identity proofing is a foundational element to enable digital financial services to function properly. This element is challenged by the proliferation of compromised personally identifiable information (PII), the increasing use of synthetic identities, and the presence of multiple, varied approaches to identity proofing. Simultaneously, technological developments are enabling dynamic identity evidence such as state mobile driver’s licenses (mDLs) or other identity credentials that are frequently updatable and interoperable, as well as behavioral analytics.”

5. With regard to biometrics, all “face recognition technology” is not the same, both in terms of how the technology works, as well as the potential biases and risks. The technical and policy issues involved in terms of a 1:1, on-device match of a face on a smartphone, for example, are wildly different from applications of face recognition technology in surveillance applications; these applications do not even share most of the same technologies. Likewise, the issues involved with both of those applications are different from those involved with the use of face recognition technology in a controlled setting when someone is applying for a driver’s license or passport, or processing through a border control checkpoint.

We have seen a number of instances where the press or policymakers have inappropriately conflated issues tied to one application of face recognition with another – for example, suggesting that problems associated with surveillance applications mean that face recognition should not be used on someone’s smartphone. It will be important for OSTP and other policymakers to ensure that any polices around the use of biometrics technology are appropriately targeted to specific applications, and the specific risks or harms associated with those applications.

6. Many of the concerns we are seeing about the use of biometrics and other AI-powered identity tools – and the policy proposals to address these concerns – are based on

\(^3\) See https://fidoalliance.org/fido-alliance-announces-id-and-iot-initiatives/
\(^4\) See https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1270-draft.pdf
\(^5\) See https://www.fdic.gov/fditech/techsprints/measuring-effectiveness.html
shortcoming on how certain products or technologies perform today in terms of accuracy or bias. However, technology is advancing rapidly, and we believe OSTP and other policymakers should be preparing for a future where some of these technologies are remarkably accurate. We are already seeing the use of next generation approaches to face liveness and face matching that do not measure refracted or reflected light, for example; this can help to address some of the accuracy struggles that earlier face biometric technologies had with some populations with darker skin.

Looking ahead 5-10 years, we believe the broader policy questions will center less around accuracy and more on the topic of “if, where, and how” AI-powered tools should or should not be used.

7. One way to explore the appropriate use of – and potential pitfalls with – AI-enabled identity tools in regulated industries is through the use of “regulatory sandboxes” established in partnership with the government. In the United Kingdom, for example, the Information Commissioner’s Office (ICO) has used sandboxes as a way to conduct research on measuring and mitigating algorithmic bias facial recognition technology. The research included best practices in data labelling, performance measurement and optimum bias mitigation techniques, all in the wider context of ensuring protection of personal data. The US, to date, has not embraced this sort of sandbox approach, but we believe it may be a promising way for government to partner with industry to address potential concerns about AI-enabled identity verification solutions.

8. The single best way to address concerns with regard to bias in AI being used in identity proofing tools is to pass the Improving Digital Identity Act of 2021. In that every product using AI to try to determine identity is trying to “guess” what, in most cases, only the government really knows. There is no better way to address concerns about probabilistic systems run amuck than to enable new deterministic systems that rely on the actual source of identity in government. America is not going to truly solve identity proofing without the kinds of identity attribute validation services that the bill calls for.

On this front, OSTP can help. The Improving Digital Identity Act is largely focused on directing the White House to establish and “Improving Digital Identity Task Force” to establish a government-wide effort to develop secure methods for Federal, state and local agencies to validate identity attributes to protect the privacy and security of individuals and support reliable, interoperable digital identity verification in the public and private sectors.

---

6 For details on one vendor’s work with the ICO, see [https://ico.org.uk/media/fororganisations/documents/2618551/onfido-sandbox-report.pdf](https://ico.org.uk/media/fororganisations/documents/2618551/onfido-sandbox-report.pdf)

The idea behind these attribute validation services is simple: Governments should modernize legacy paper-based identity systems around a privacy-protecting, consumer-centric digital model that allows consumers to ask the agency that issued a credential to stand behind it in the online world—by validating the information from the credential. The Social Security Administration (SSA) and state governments—the latter in their role as issuers of driver’s licenses—are the best positioned entities to offer these services to consumers.

While the White House could wait for Congress to direct it to establish this Task Force, a better choice would be for the White House to establish such a Task Force through executive action, such as an Executive Order.

By leading a drive in the White House to directly tackle digital identity challenges, OSTP can help develop new identity solutions that can address concerns about bias in AI-powered tools.

Note that this idea is not new: it was embraced in the 2016 report from the bipartisan Commission on Enhancing National Cybersecurity, which, in response to the wave of attacks leveraging compromised identities, set a clear goal for the country: “The Commission believes that the shared goal of both the public and private sectors should be that compromises of identity will be eliminated as a major attack vector by 2021.”

As a key element of this action item, the Commission stated: “The government should serve as a source to validate identity attributes to address online identity challenges.”

Per the report: “The next Administration should create an interagency task force directed to find secure, user-friendly, privacy-centric ways in which agencies can serve as one authoritative source to validate identity attributes in the broader identity market. This action would enable government agencies and the private sector to drive significant risk out of new account openings and other high-risk, high-value online services, and it would help all citizens more easily and securely engage in transactions online.

“As part of this effort, the interagency task force should be directed to incentivize states to participate. States—by issuing drivers’ licenses, birth certificates, and other identity documents—are already playing a vital role in the identity ecosystem; notably, they provide the most widely used source of identity proofing for individuals. Collaboration is
key. Industry and government each have much to gain from strengthened online identity proofing.

“The federal government should support and augment existing private-sector efforts by working with industry to set out rules of the road, identify sources of attributes controlled by industry, and establish parameters and trust models for validating and using those industry attributes.”

Government should act on this recommendation, with a particular focus on having the Federal government:

1) Establish the interagency task force called for by the Commission to identify how government agencies can offer these services. We believe OSTP can play a leadership role here, in conjunction with OMB and the National Security Council.

2) Lead development of a framework of standards and operating rules to make sure this is done in a secure, privacy-preserving way. NIST is in an ideal position to lead here.

3) Identify any legal or regulatory barriers that Federal or state agencies need to address to enable these services.

4) Fund work to get it started. We note that the GSA has for some time had an office in its Technology Transformation Service (TTS) to support better government-wide approaches to identity proofing. This office should be fully funded and empowered to drive action across government.

This idea was endorsed in policy in 2019 when the Office of Management and Budget (OMB) issued M-19-17,9 which stated:

“Agencies that are authoritative sources for attributes (e.g., SSN) utilized in identity proofing events, as selected by OMB and permissible by law, shall establish privacy-enhanced data validation APIs for public and private sector identity proofing services to consume, providing a mechanism to improve the assurance of digital identity verification transactions based on consumer consent.

“These selected agencies, in coordination with OMB, shall establish standard processes and terms of use for public and private sector identity proofing services that want to consume the APIs.”

Despite this OMB memo, little has taken place since then to advance these attribute validation initiatives. To the extent there are concerns about the overuse of AI in

---

identity verification, this is the single most meaningful step the government could take to address these concerns.

II. How AI is being used in identity today

At a high level, there are two core challenges we are trying to solve in digital identity:

1. Identity Proofing and Verification – figuring out whether someone is who they claim to be at account opening. Exploiting weaknesses in our identity proofing infrastructure is what has allowed criminals to steal tens of billions of dollars from state unemployment insurance (UI) programs, as well as commercial firms in financial services, retail, and other sectors.\(^\text{10}\)

2. Authentication – Once an account has been created, how do you create systems that can securely log customers in to or recover that account? This has become quite important in a world where passwords just don’t cut it anymore, and cybercriminals are exploiting the weaknesses of passwords and other weak authentication tools to launch billions of attacks each day.

These challenges align with the way that NIST has broken down its guidance on digital identity. Identity Proofing and Verification is covered by NIST in SP 800-63A while Authentication is covered in SP 800-63B.\(^\text{11}\)

On the Identity Proofing and Verification side, there are two primary use cases where AI and machine learning (ML) play an important role:

1. Remote ID proofing tools that ask a consumer to take a photo of their ID (such as a driver’s license), as well as a selfie picture. In many of these products, AI/ML is used to help validate whether an ID document is real or counterfeit, as well as whether the selfie matches the photo on the ID. The role of AI/ML in these products is generally one where they “study” different documents and “learn” over time how to better tell a real driver’s license or passport from a fake.

In addition, AI/ML is also often used in the biometric aspects of the products, such as facial comparison and matching. Here, we are starting to see some firms address concerns about ways to spoof “liveness” of faces – as well as the accuracy and consistency of some weaker face matching algorithms – by shifting to algorithms based on 3D models of faces, rather than traditional 2D photos.


It is worth noting that Congress recognized the importance of these solutions in financial services in 2018 when it passed the Economic Growth, Regulatory Relief, and Consumer Protection Act. Section 213 of that bill was called the Making Online Banking Initiation Legal and Easy (MOBILE) Act, and it preempted some state laws that prevented banks from scanning a driver’s license to support mobile applications for new accounts.

Today, the types of solutions detailed in the MOBILE Act are widely used – but not all of them use AI, and performance of the products is inconsistent between vendors. In general, we have seen that the products that have an AI component are more accurate than those that do not.

As we noted earlier, one organization has launched an initiative to test and certify these solutions, with a focus on establishing performance criteria for these products and partnering with a number of independent testing labs to measure whether products meet these performance criteria. To the extent that there is a concern that AI or ML technology used in some of these products might not measure up, new testing and certification programs like these will be a major asset. Many vendors are saying “trust us, our products work” – certification programs will verify that they actually do.

2. Data-centric approaches to ID proofing that improve accuracy through use of AI. Here, vendors in the space look at many different signals and data sources, and use AI to help predict over whether an applicant might be fraudulent or not – analyzing data and signals with algorithms that are constantly evolving and improving thanks to AI and that help companies root out fraud, including synthetic identity fraud, and make more accurate decisions.

Signals and data sources may include what can be inferred about a device being used to apply for an account, or the way a user interacts with that device as they enter their information digitally. Examining a wider set of signals and data sources provides a multi-dimensional view of identity for enriched verification, and simultaneously allows vendors and implementers to identify patterns of repeated identity fraud across government agencies and the private sector driven by sophisticated crime rings. Given that it is these crime rings that were at the heart of much of staggering identity fraud losses in the past year, this is an increasingly important use of AI.

Overall, many of our members in the financial services space report that without AI/ML and risk-based models it would be impossible to approve as many applications for financial services or catch as much fraud.

---

12 See Public Law 115-174
13 See https://fidoalliance.org/fido-alliance-announces-id-and-iot-initiatives/
14 An excellent summary of losses to government agencies was conducted by the Pandemic Response Accountability Committee (PRAC) https://www.pandemicoversight.gov/our-mission/identity-theft-in-pandemic-benefits-programs
On the Authentication side, AI and ML also play an important role as part of “authentication analytics” solutions that look at dozens of different data points and signals about how an individual is 1) trying to authenticate or 2) interacting with a device or application after initial authentication. These include both “behavioral biometrics” tools as well as tools that look at other data points.

AI has become increasingly important as adversaries focus on compromising authentication credentials to execute cyber attacks.\(^{15}\)

Here, we are seeing firms in financial services and other sectors use tools that look at data such as behavior, location, typing pattern, access requests (i.e., a record of trying to get to something they should not have access to), etc. The tools then study all these elements and then use AI to make a prediction as to whether anything seems “off” or shows a sign of account or device compromise.

By pairing more traditional authentication with analytics solutions that use AI to “score” in real time the likelihood that an account remains in the hands of its rightful owner, we are closer than ever to eliminating reliance on passwords and blocking credential-focused cyber-attacks.

The emergence of reliable authentication analytics tools is contributing to the rise of a new model for authentication called “continuous, risk-based authentication.” Here a traditional authentication factor like a password or MFA is paired with analytics tools that analyze different signals. Some might automatically remediate a sign of fraud by refusing authentication, in other cases it might trigger a signal that is then used to ask a user for additional factors of authentication. To be clear, not all of these tools use AI, but many do.\(^{16}\)

As major banks and cloud providers see tens or hundreds of millions of fraudulent attacks each day on their login systems, AI has emerged as an essential tool to detect and block them.

We greatly appreciate OSTP’s willingness to consider our comments and suggestions and welcome the opportunity to have further discussions. Should you have any questions on our feedback, please contact the Better Identity Coalition’s coordinator, Jeremy Grant, at [email protected] or [email protected].

---

\(^{15}\) The Cybersecurity and Infrastructure Security Agency (CISA) at DHS has flagged these concerns multiple times (see https://www.cisa.gov/uscert/ncas/analysis-reports/ar20-268a) and the White House has made stopping attacks on compromised credentials a centerpiece of its new Federal Zero Trust Strategy (see https://zerotrust.cyber.gov/federal-zero-trust-strategy/).

\(^{16}\) This model of “continuous authentication” was highlighted in a paper last year published by the Health-ISAC. https://h-isac.org/wp-content/uploads/2021/02/H-ISAC_All-About-Authentication-White-Paper.pdf