Atlantic Council
SCOWCROFT CENTER
FOR STRATEGY AND SECURITY

ISSUE BRIEF

# Biometrics at the Border: Balancing Security, Convenience, and Civil Liberties

JANUARY 2022 SETH STODDER AND THOMAS S. WARRICK

The **Scowcroft Center for Strategy and Security** works to develop sustainable, nonpartisan strategies to address the most important security challenges facing the United States and the world. The Center honors General Brent Scowcroft's legacy of service and embodies his ethos of nonpartisan commitment to the cause of security, support for US leadership in cooperation with allies and partners, and dedication to the mentorship of the next generation of leaders.

The Atlantic Council's ***Forward* Defense (*FD*)** practice shapes the debate around the greatest defense challenges facing the United States and its allies, and creates forward-looking assessments of the trends, technologies, and concepts that will define the future of warfare. Through the futures we forecast, the scenarios we wargame, and the analyses we produce, *FD* develops actionable strategies to help the United States navigate major power conflict and defend forward, alongside allies and partners. As the character of war rapidly changes, *FD* assesses the operational concepts and defense industrial tools necessary to effectively deter and defend against emerging military challenges

We are all individuals—"one, but not the same," according to U2's classic song.[1] We each have our own faces, DNA, fingerprints, and iris patterns, all of which can be recorded objectively and individually. Often referred to as "biometrics," these attributes can be used to prove we are who we say we are. They can also track where we have been or where we may be going.

The use of fingerprints for identification dates back more than two thousand years, and their use by law enforcement to solve crimes dates back to the 1880s.[2] The predecessor of the Federal Bureau of Investigation (FBI) set up its first fingerprint database, on paper cards, in 1924.[3] Ever since then, the analysis of fingerprints, facial images, and other biometric identifiers has been a key tool relied upon by police officers around the world. Border agencies also collect biometrics from people they encounter, analyzing them to confirm the identity and admissibility of those seeking to enter or exit a country. US laws passed in 2002 and 2004—after the September 11, 2001, terrorist attacks—required the US Departments of State (DOS) and Homeland Security (DHS) to fingerprint all foreign travelers to the United States.[4]

1 U2, "One (Official Music Video)," YouTube, December 14, 2019, https://www.youtube.com/watch?v=ftjEcrrf7r0.

2 Jeffrey G. Barnes, "History" in *The Fingerprint Sourcebook* (Washington, DC: US Department of Justice, 2012), https://www.ojp.gov/pdffiles1/nij/225321.pdf.

3 Ibid.

4 Marcy Mason, "Biometric Breakthrough," US Customs and Border Protection, last visited January 11, 2022, https://www.cbp.gov/frontline/cbp-biometric-testing.

In 2022, however, border agencies around the world are using biometrics in a different way. Working in partnership with airlines, airports, cruise ships, and individual travelers, agencies like US Customs and Border Protection (CBP) and the UK Border Force have realized that biometrics—in particular, facial recognition—can be used not only for screening and enforcement, but also to expedite the secure, lawful movement of people and goods across borders, through airports, and throughout global transport networks. Government agencies and private industry are beginning to use this technology to develop and deploy "smart borders," to both increase security and process lawful trade and travel faster than before.

But, these advances do not come without risk. Facial recognition enables convenience, but it can also unlock the door to the type of persistent surveillance that autocratic states like China and Russia regularly employ to repress dissent. In the United States, this triggers images of nightmarish science-fiction dystopias like that seen in *Minority Report*.[5] Also, the more data the government collects, the more everyone's personal lives become vulnerable to cyber hackers and identity theft. And, what if the facial matching algorithms get it wrong? Are people stuck like Walter Child in Gordon Dickson's *Computers Don't Argue* or Archibald Buttle in the movie *Brazil*, unable to prove to skeptical government officers that they are who they say they are?[6] Given the documented racial, ethnic, and gender biases in many facial-recognition systems, how often do mistakes happen, and are they systematic rather than random—effectively prejudiced against communities of color?[7]

This Issue Brief provides a primer on these questions, summarizing how biometrics are currently being used at the borders, addressing the risks, and recommending a path forward.

## BIOMETRICS AND THE BORDERS—1.0

Since 1994, the US Border Patrol—now part of CBP within DHS—has collected fingerprints from the migrants it apprehends, entering them into the Automated Biometric Identification System (IDENT). The IDENT system allows Border Patrol agents to identify migrants previously encountered or apprehended. By running the fingerprints through the FBI's Next Generation Identification (NGI) system, CBP can also quickly determine whether encountered individuals have criminal records. More recently, CBP and Homeland Security Investigations (HSI), part of US Immigration and Customs Enforcement (ICE), have begun to use DNA analysis to determine whether migrant children are actually related to the adults who claim to be their parents when crossing the border, or whether the kids are in fact victims of human trafficking—an effort ICE has called "Operation Double Helix."[8]

CBP also collects fingerprints and photographs of non-US persons entering the United States at official Ports of Entry—in fiscal year 2019 alone, from approximately *seventy-nine million* foreign nationals. CBP initially compares a traveler's identity to existing US government photo and fingerprint holdings. If the person is a first-time Visa Waiver Program (VWP) traveler (i.e., someone with no prior entry or visa, so no prior fingerprint or

5 Andrew Liptak, "Minority Report Holds Up Because It's About Surveillance, Not Gadgets," *Verge*, June 30, 2017, https://www.theverge.com/2017/6/30/15865462/minority-report-steven-spielberg-surveillance-technology.

6 Gordon R. Dickson, "Computers Don't Argue," *Analog Science Fiction—Science Fact*, September 1965, partially reprinted in David H. Ahl, ed., *The Best of Creative Computing*, 2, 1977, https://archive.org/details/bestofcreativeco00ahld/page/133/mode/2up; Claire Suddath, "Top 10 Movies That Mess with Your Mind," *Time*, July 15, 2010, https://entertainment.time.com/2010/07/16/top-10-movies-that-mess-with-your-mind/slide/brazil/.

7 Alex Najibi, "Racial Discrimination in Face Recognition Technology," Harvard University Graduate School of Arts and Sciences, October 4, 2020, https://sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology/.

8 *The Exploitation of Migrants Through Smuggling, Trafficking, and Involuntary Servitude*, Senate Homeland Security and Government Affairs Committee (2019), (testimony of Gregory C. Nevano), 3–4, https://www.hsgac.senate.gov/imo/media/doc/Testimony-Nevano-2019-06-26.pdf.

photo capture by the US government), CBP will collect biometrics for the traveler, and will also do a one-to-one match of the traveler to the photo in their passport.

Many other countries also collect biometrics at the borders, or are developing systems to do so. For example, the European Union (EU) this year will begin deploying its new Entry/Exit System (EES) to collect fingerprints and facial images from non-EU nationals crossing the external borders of the Schengen Area, and Canada is also quickly developing a similar system for its borders.[9] Many Middle Eastern countries currently collect iris scans, an increasing number also collect fingerprints and photographs, and Israel recently approved a law that would require collection of fingerprints and photos of all non-Israelis arriving in the country.[10] In short, biometric collection and verification are becoming as routine as checking a government-issued passport.

## BIOMETRICS 2.0: ADVANCING SECURITY WHILE SPEEDING UP LEGITIMATE TRADE AND TRAVEL

Biometrics are useful not only for security—advancing society's interest in protecting itself from threats—but also for significantly increasing the speed through which people and goods cross the border. Everyday life illustrates this convenience: look into the camera of your iPhone or computer, and it recognizes your face and unlocks itself. The convenience factor is multiplied manyfold at the border, where—given the huge volume of travel and trade—even the shortest delays spent with an officer manually checking documents can quickly multiply into seemingly endless lines of grumpy, dehydrated, and exhausted travelers snaking deeply back into the corridors of a crowded international air terminal—an irritating situation made dangerous in the era of COVID-19 and other airborne pathogens. Biometrics are helping cut these lines and, in the process, are transforming how travelers move through checkpoints and board planes—getting people where they want to go faster and with less hassle, while also improving security by better detecting imposters and others whose entry or exit must be controlled.

Two decades ago, the first commissioner of CBP after its creation, Robert Bonner, spoke of the need to achieve the "twin goals" of *security* and the *facilitation* of lawful travel and trade.[11] This vision arose from the searing experience of the days after 9/11, when strict border security measures resulted in massive twelve-to-fourteen-hour traffic jams at both the US-Canada and US-Mexico borders, disrupting "just-in-time" supply chains, shutting down cross-border trade, and disrupting other parts of the North American economy that depended on cross-border trade. Bonner's challenge was to work with foreign partners and the private sector to quickly reinvent processes at the borders to achieve the necessary security without impeding the swift flow of lawful travel and commerce so vital to the US economy.

CBP adopted an integrated strategy of risk management, consisting of three core elements: the collection and analysis of information on travelers and trade to assess risks and spot the "needles" in the vast "haystack" of cross-border travel and trade; the deployment of scanning technology to spot hidden weapons or other dangerous things; and close collaboration with foreign partners and the global private sector to secure shared borders and, more importantly, the global systems of transportation and trade—in essence, making the entry and exit points into and out of global transportation and trade networks effectively the "borders" that CBP and its foreign and private-sector counterparts needed to secure.

This post-9/11 risk-management strategy succeeded dramatically in reducing the threat from global terrorist groups, through such US initiatives as the Customs-Trade Partnership Against Terrorism (C-TPAT), the creation of the National Targeting Center (NTC) to analyze data on travelers and cargo in order to assess risk, and the Smart Border Accords with Mexico and Canada, among others. These efforts were supplemented by global initiatives like the World Customs Organization's SAFE Framework of Standards to Secure and Facilitate Trade and the United Nations (UN) Security Council's Resolution 2178 (2014), which then-President Barack Obama pushed the world to adopt in response to the rise of the Islamic State of Iraq

9 "Entry/Exit System (EES)," European Commission, last visited January 15, 2022, https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/smart-borders/entry-exit-system_en; Jim Bronskill, "Feds Planning to Use Biometrics at Canada-U.S. Border," *Canada's National Observer*, June 8, 2021, https://www.nationalobserver.com/2021/06/08/news/feds-plan-biometrics-canada-us-border-COVID-identificaton.

10 Frank Hersey, "Israel Could Capture Biometrics of All Non-Citizens Entering the Country," BiometricUpdate.com, August 2, 2021, https://www.biometricupdate.com/202108/israel-could-capture-biometrics-of-all-non-citizens-entering-the-country.

11 "Remarks of Commissioner Robert C. Bonner," Trade Support Network (TSN) Conference, July 7, 2004, https://cscb.ca/article/remarks-commissioner-robert-c-bonner.

and al-Sham (ISIS) and the threat presented by foreign terrorist fighters. UN Security Council Resolution 2396 (2017) advanced these standards further during the Donald Trump administration. Because of these and other national and global measures, international travel and trade are now demonstrably safer than they were in 2001.

But, crucially, the risk-management strategy has also resulted in the more efficient movement of lawful travelers and commerce across national borders. For example, because CBP collects and analyzes Advance Passenger Information (API) and Passenger Name Record (PNR) data on air passengers before a plane overseas departs for the United States, CBP can perform security checks and assess whether individual travelers present any risk well before the travelers depart a foreign location. Because the vast majority of travelers present little or no risk, most pass relatively unimpeded through border checkpoints and are quickly sent on their way. Millions of travelers also voluntarily participate in CBP's Global Entry, the Transportation Security Administration's (TSA) PreCheck, or similar "trusted traveler" programs of other countries, which permit a traveler to provide information well in advance to the government agency, allowing it to perform a thorough background check to determine if the traveler is sufficiently low risk that they become eligible for a "fast lane" through immigration, customs, or security formalities. Biometrics—both fingerprints and digital photo images—are key to these trusted-traveler programs, verifying that travelers are who they and their travel documents say they are.

## BIOMETRICS 3.0: THE NEXT STEP—FACIAL BIOMETRIC TECHNOLOGY

Technological advancements in biometrics—in particular, automated facial biometric comparison—have the potential to make international travel and trade even easier. CBP and its counterparts elsewhere are today working in partnership with airlines and airports (as well as cruise-ship operators and seaports) to employ facial-comparison capabilities to make cross-border travel and trade more seamless, efficient, and secure.

In the United States, this started, in large part, because of the need to implement the long-standing congressional mandate to collect biometrics on all foreign nationals *exiting* the United States. But, of course, talk was cheap. While Congress mandated "biometric exit," for many years it did not appropriate the billions of dollars needed to redesign US international air terminals to accommodate the necessary checkpoints, equipment, and security personnel. And, DHS was given no magic wand. Biometric exit became a looming logistical and financial nightmare hanging over state and local airport authorities, with no particular plan for how it would happen. This began to change, however, in Fiscal Year 2016, when Congress finally gave CBP up to $100 million a year for ten years to establish biometric exit, and CBP launched a pilot version of what would become the Traveler Verification System (TVS). In 2017, then President Donald Trump issued an executive order directing DHS to expedite implementation.[12] In the process of carrying out President Trump's direction, though, CBP quickly realized its TVS pilot was more than just the grudging implementation of a congressional mandate—it was the future of cross-border travel. CBP realized it could offer "identity as a service" to its air-travel stakeholders (and, ultimately, to TSA) wherever identify verification is required, including at check-in, bag drop, security checkpoint, and departure.

Under the traditional system, travelers boarding a plane departing the United States show their passports to airline personnel, who then look at them and electronically scan the documents before allowing the travelers on board. TVS automates that process by, instead, taking a digital photo of the traveler before boarding and using a high-performing facial-recognition algorithm to instantaneously compare it to a database of existing passport or visa photos of all travelers on that flight's manifest. In some airports (those where airlines employ an "e-gate"), if a traveler's photo matches, the boarding gate opens automatically. In others, the traveler gets the green light from a totem camera, which signals the traveler to walk onto the plane. Either way, the identity comparison and verification are automated and instantaneous—and some airlines have chosen to expedite things even further by using the TVS process not only to obviate the need for manual passport checks, but to do the same for boarding passes. If the photo does not match, however, things revert to the old system, with CBP or airline personnel performing a manual identity check of the traveler's passport. For US citizens, the TVS process is entirely voluntary; they can always choose to have their passports reviewed manually, in the old-school style.

For travelers entering the United States, CBP utilizes "Simplified Arrival," a primary processing application that leverages the TVS facial-comparison system. Photos are taken when the traveler reaches primary inspection, and the process is similarly voluntary for US citizens and some categories of non-US

12 "Executive Order No. 13769: Protecting the Nation from Foreign Terrorist Entry into the United States," Executive Office of the President, January 27, 2017, https://www.federalregister.gov/documents/2017/02/01/2017-02281/protecting-the-nation-from-foreign-terrorist-entry-into-the-united-states.

citizens. Thus, the computerized checks at departure and arrival generate the necessary biometric photographic match to satisfy the long-standing requirements of biometric entry and exit for most non-US travelers. While there is a cost to installing and operating the system, it is small compared to redesigning all US-based international air terminals—and it is done in full partnership with private-sector stakeholders. Years of testing have demonstrated that the expansion of biometric facial-comparison technology through these kinds of public-private partnerships is the most secure, efficient, and cost-effective way to fulfill the congressional mandate while protecting the privacy of all travelers.

The TVS system is now utilized at two hundred and five US entry airports, thirty-two US departure airports, thirteen seaports, all CBP preclearance stations overseas, and almost all pedestrian- and bus-processing facilities on the land borders.[13] CBP is also piloting the system for land-border vehicle traffic, and is also working with TSA to pilot the system for PreCheck.[14] CBP says that, from the launch of the TVS tool in June 2017 to January 2022, it has processed more than one hundred and thirty million passengers with the biometric facial-comparison technology across all modes of travel, which has proven 98 to 99 percent accurate in terms of verifying identity.[15] As a result, CBP has intercepted more than *two thousand* imposters seeking to enter the United States under false pretenses.[16]

The new system has proven extremely popular with airlines, airports, and travelers, for the simple reason that it makes traveling through airports so much easier and faster. By eliminating the need for manual document checks, the use of facial biometrics for identity verification shortens the time it takes to board a plane or clear traditional processing. Travelers can, therefore, choose whether to arrive later, spend more time shopping, or get to their airline seats faster, with less time waiting in long immigration-processing lines.

Similar systems are being deployed around the world. As noted previously, the EU is deploying its similar Entry/Exit System this year. The United Kingdom has gone further, using facial recognition at multiple points at Heathrow Airport—check-in, baggage drop, security, and boarding—to provide a "seamless experience for passengers" by allowing them to move unhindered through the airport. Other countries, including France and Australia, are also walking down the same path.

## CONCERNS RAISED ABOUT THE USE OF BIOMETRICS AT THE BORDER

In November 2020, CBP published a proposed rule to expand biometric processing to all non-US citizens and remove port limitations on the use of biometrics in the exit environment.[17] The proposal has drawn a flurry of comments, both pro and con, and the Joseph Biden administration—after extending the comment period to March 2021—is still considering whether to issue a final rule.[18] A number of privacy and immigrant-advocacy organizations—including the Electronic Privacy information Center (EPIC), the Center for Democracy and Technology (CDT), the American Civil Liberties Union (ACLU), and others—have raised objections to the continuation of CBP's use of facial biometrics.[19]

### 1 Fear of a Surveillance State

The broadest objection is that facial recognition is an "inherently dangerous technology," and that CBP's use of it could be the beginning of a slippery slope that could lead to more generalized tracking of both Americans and non-US persons, not only at the borders, but also within the United States—rais-

13 "Introducing Biometric Facial Comparison," US Customs and Border Protection, https://biometrics.cbp.gov/.

14 "TSA-CBP Biometric Technology Pilot for Trusted Travelers," US Transportation Security Administration, January 15, 2021, https://www.tsa.gov/sites/default/files/tsa-cbp_phaseiii_pilot_one-pager_clean_1-15-21.pdf.

15 "Introducing Biometric Facial Comparison."

16 "CBP Expands Simplified Arrival in Washington," US Customs and Border Protection, June 30, 2021, https://www.cbp.gov/newsroom/local-media-release/cbp-expands-simplified-arrival-washington.

17 "Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States," US Customs and Border Protection, November 19, 2020, https://www.federalregister.gov/documents/2020/11/19/2020-24707/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states.

18 "Collection of Biometric Data from Noncitizens Upon Entry to and Exit from the United States," Executive Office of the President, Fall 2021, https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=1651-AB12.

19 "EPIC Urges CBP to Halt Use of Facial Recognition for Biometric Entry/Exit," Electronic Privacy Information Center, December 21, 2020, https://epic.org/epic-urges-cbp-to-halt-use-of-facial-recognition-for-biometric-entry-exit/; Greg Nojeim and Mana Azarmi, "CDT Submits Supplemental Comment in Opposition to DHS Collection of Biometric Data from Aliens Upon Entry to and Departure from U.S.," Center for Democracy and Technology, March 11, 2021, https://cdt.org/insights/cdt-submits-supplemental-comment-in-opposition-to-dhs-collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-u-s/; "Email to Secretary Alejandro Mayorkas, Re: 85 Fed. Reg. 74162, Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States," American Civil Liberties Union, March 10, 2021, https://cdt.org/wp-content/uploads/2021/03/2021-03-10-Letter-to-DHS-re-Face-Surveillance-nprm-final.pdf.

ing the specter of a *Minority Report*-style surveillance state.[20] Some also say that the use of such technology at the border dangerously singles out immigrants, given that most non-US persons cannot opt out of CBP using it to process their entry.[21] Photos of in-scope non-US travelers are enrolled and retained in IDENT for up to seventy-five years. (CBP deletes its copies of all photos, within twelve hours for US citizens and fourteen days for all others.) Objectors express the fear that such images might be shared with US or foreign law enforcement.

These are serious concerns, but CBP is utilizing this technology in relation to crossings of the US border, where the US Supreme Court has consistently recognized that "the Government's interest in preventing the entry of unwanted persons and effects is at its zenith," that the government has "plenary power to make rules for the admission of aliens," and that CBP has broad authority under the Fourth Amendment to search and question all seeking admission or return to the United States.[22] Moreover, DHS has been collecting biometrics—both fingerprints and photographs—from non-US persons for many years through the US-VISIT system. The State Department already issues passports to US citizens and machine-readable visas for non-US citizens, both of which now include biometric photographs. And, all federal law-enforcement agencies, including CBP, regularly cooperate with foreign, state, local, and tribal authorities by sharing biographic and biometric data on individuals—including photos—where there is good cause and it is permitted by law. Fundamentally, the use of TVS does not change or add much to the information already possessed by the government. It takes one additional photo and compares it to information that already exists in government databases, all pursuant to a long-standing congressional mandate and consistent with broad border authorities recognized by the Supreme Court for more than a century.

The question of whether facial comparison is an "inherently dangerous" technology is a debatable one—especially given its ubiquity (look at your iPhone or Android). But, its use by repressive, authoritarian regimes demonstrates the risks, so careful safeguards governing how CBP uses facial-comparison technology or shares images are clearly appropriate—and many already exist. As required by law, CBP has published a Privacy Impact Assessment discussing the program in great detail, and it has provided notice of how it shares data in the various System of Records Notices (SORNs) it also publishes, as well as in the proposed rule.[23] Additionally, CBP provides notice to travelers through message boards or signs, as well as verbal announcements in some cases, to inform the public that CBP or a stakeholder will be taking photos for identity-verification purposes. In addition to CBP's own internal oversight and officer-training protocols, DHS also provides oversight through its Offices of Civil Rights and Civil Liberties (CRCL) and Privacy, as does the Privacy and Civil Liberties Oversight Board (PCLOB). That said, more safeguards could and should be put in place. In 2020, the Biometrics Subcommittee of the Homeland Security Advisory Council (HSAC) issued a report analyzing DHS biometrics programs and recommending the creation of a DHS Biometrics Oversight and Coordination Council (BOCC), chaired by the DHS deputy secretary, as well empowering the DHS Office of Strategy, Policy and Plans to lead the development of DHS-wide policies on biometrics, including on such issues as retention and sharing.[24] The HSAC's recommendations regarding additional oversight structures are sensible, and should be implemented.

Ideally, current limits on CBP broadening use of the technology or sharing facial-biometric data should not be waivable by executive action alone. This is an area in which congressional action can provide additional checks against the misuse of data or technology.

## 2 Data Protection

Others have argued that CBP's use of facial biometrics should be terminated because CBP will be unable to protect the biometric data from cyber hacks—citing the 2015 example of the Office of Personnel Management being unable to protect its

20 "Comments of the Electronic Privacy Information Center," Electronic Privacy Information Center, December 21, 2020, https://epic.org/wp-content/uploads/apa/comments/EPIC-Comments-CBP-Biometric-Entry-Exit-December-2020.pdf.

21 "Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States; Re-Opening of Comment Period," US Customs and Border Protection, February 10, 2021, https://www.federalregister.gov/documents/2021/02/10/2021-02699/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states.

22 United States v. Flores-Montano, 541 U.S. 149, 152 (2004); Kleindienst v. Mandel, 408 U.S. 753, 766 (1972); United States v. Flores-Montano, 541 U.S. at 152-153 (citing United States v. Ramsey, 431 U.S. 606, 616 (1977)).

23 Colleen Manaher and Philip S. Kaplan, "Privacy Impact Assessment for the Traveler Verification Service," US Department of Homeland Security, November 14, 2018, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

24 "Final Report of the Biometrics Subcommittee," Homeland Security Advisory Council, November 12, 2020, https://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp056-tvs-february2021.pdf.

information from Chinese exfiltration.[25] But, for the most part, this argument is not specific to CBP. Instead, it argues that the federal government should not collect personal data at all because it cannot protect it with certainty. Protecting databases from cyber hacks requires adequate resources, oversight, accountability, and expertise, but it is not an impossible task—and restricting government agencies (or private-sector entities) from collecting personal data required to perform their functions is an obvious non-starter. Strong governance and oversight are a more sensible position, and the HSAC report's recommendation of a DHS BOCC providing strong, senior-level oversight for TVS and other DHS biometrics programs is a good one, as is the HSAC's additional recommendation that the Cybersecurity and Infrastructure Security Agency (CISA) play a key role in the protection of data. Furthermore, nothing comes for free, so Congress needs to ensure that federal agencies have the cybersecurity resources, personnel, and authorities to do the job.

## 3 Accuracy and Bias

Finally, some assert that the 98–99-percent accuracy rate for CBP's Biometric Facial Comparison Technology is not good enough, and that—given the huge volume of travelers—many people will suffer from erroneous "no-match" determinations. But, the obvious answer to this is that, at an airport, the consequence of a no-match decision is simply that a CBP officer or airline official will need to perform an old-school manual check of the traveler's passport or visa. This may cause a minute's inconvenience, but automated checks that work 98 to 99 percent of the time will significantly reduce the number of travelers whose documents need a manual check. Moreover, CBP has processed more than one hundred and thirty million people through the system since 2017 and, thus far, mistaken "no-match" incidents have not arisen as a major issue. On the contrary, facial-comparison technology has proven *more* accurate than manual document checks, as evidenced by the more than *two thousand* imposters the system has enabled CBP to catch

A related objection is that the use of some facial-recognition technology algorithms has resulted in bias against persons of color. But, the National Institute of Standards and Technology (NIST), which performed the much-reported study indicating that *some* facial-recognition algorithms can produce biased results, actually found that the facial-recognition algorithm specifically used by CBP for facial comparison in TVS—NEC-3 (developed by NEC Corporation)—is highly accurate.[26] As noted in the NIST study, some facial-recognition algorithms are better than others, and the bad ones are indeed more likely to produce demographically biased results.[27] But, the best ones—like the NEC-3 algorithm used by CBP—are highly accurate and do not "display a significant demographic bias."[28] CBP officials have also told Congress that "CBP's operational data demonstrates that there is virtually no measurable differential performance in matching based on demographic factors."[29] CBP continues to conduct analysis, as well as monitor algorithm performance and technology enhancements, to ensure a high biometric performance.

Nevertheless, CBP is focused on this issue, as it must be, and careful oversight by existing bodies like the Office of Civil Rights and Civil Liberties, and by the new DHS BOCC recommended by the HSAC Biometrics Subcommittee, is vital here, as is full transparency to these institutions, Congress, and the general public.[30] This should provide a measure of confidence that CBP's algorithms will continue to improve, avoid any appearance of unfair bias, and will become even more accurate over time.

---

25 "Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States: Docket No. USCBP-2020-0062," US Department of Homeland Security, https://public-inspection.federalregister.gov/2020-24707.pdf.

26 Aaron Boyd, "CBP is Upgrading to New Facial Recognition Algorithm in March," Nextgov, February 7, 2020, https://www.nextgov.com/emerging-tech/2020/02/cbp-upgrading-new-facial-recognition-algorithm-march/162959/; "Face Recognition Vendor Test Part 3: Demographic Effects," National Institute of Standards and Technology, December 2019, 8, https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf#page=11. Note that the NEC-3 algorithm "is on many measures, the most accurate we have evaluated." See also: "Final Report of the Biometrics Subcommittee," Homeland Security Advisory Council, November 12, 2020, 26–32.

27 "Face Recognition Vendor Test Part 3," 2. Note that error rates vary depending on the algorithm, "with the most accurate algorithms producing many fewer errors," with these more accurate algorithms "expected to have smaller demographic differentials."

28 Michael McLaughlin and Daniel Castro, "The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist nor Sexist," Information Technology & Innovation Foundation, January 27, 2020. See also: "Face Recognition Vendor Test Part 3," 6. "More accurate algorithms produce fewer errors, and will be expected therefore to have smaller demographic differentials."

29 Boyd, "CBP Is Upgrading to a New Facial Recognition Algorithm in March."

30 "Final Report of the Biometrics Subcommittee."

## RECOMMENDATIONS AND NEXT STEPS

CBP's use of biometrics at the border has proven to be an essential tool in achieving the "twin goals" of security and the facilitation of lawful travel and trade. Accordingly, the following steps are recommended.

**Recommendation #1:** The Biden administration should continue with CBP's facial-biometrics program and, after fully considering the various public comments, move to finalize the CBP proposed rule close to the form in which it was issued in November 2020.

**Recommendation #2:** CBP should work to continue improving its facial-comparison service, and continue working with TSA to utilize facial-comparison technology for TSA's PreCheck program. CBP should continue its technical demonstration of Simplified Arrival for vehicle traffic entry at land borders.

**Recommendation #3:** DHS should carefully consider and adopt most of the recommendations of the HSAC Biometrics Subcommittee, particularly the creation of the DHS BOCC, which should be chaired by the DHS deputy secretary. DHS should empower the DHS Office of Strategy, Policy, and Plans to lead the development of DHS-wide policies on biometrics, including on such issues as retention, sharing, and—in conjunction with the DHS Office of Civil Rights and Civil Liberties—the avoidance of unfair bias against communities of color and others.

**Recommendation #4:** DHS and CBP should expeditiously move to spend the funds appropriated in the bipartisan Infrastructure Investment and Jobs Act, which will allow for expansion of biometrics capabilities at the borders.[31] Congress should also appropriate sufficient funds for operations of biometrics systems, which is a major concern today, given the huge operational challenges CBP currently faces at the border.

## ABOUT THE AUTHORS

**Seth Stodder** is a nonresident senior fellow in the *Forward* Defense practice of the Atlantic Council's Scowcroft Center for Strategy and Security. Stodder served in the Obama administration as assistant secretary of homeland security for borders, immigration, and trade policy, as well as assistant secretary of homeland security for threat prevention and security policy.

**Thomas S. Warrick** is a nonresident senior fellow in the *Forward* Defense practice of the Atlantic Council's Scowcroft Center for Strategy and Security and director of its Future of DHS Project, as well as a senior advisor with the Council's Middle East Programs. Warrick worked for the Department of Homeland Security for more than ten years, concluding his service as deputy assistant secretary for counterterrorism policy in June 2019.

## ACKNOWLEDGMENTS

This issue brief was made possible with the generous support of SAIC.


31 "Infrastructure and Jobs Act," 117th Congress of the United States, January 3, 2021, https://www.congress.gov/117/bills/hr3684/BILLS-117hr3684enr.pdf.

# Atlantic Council Board of Directors

The Atlantic Council is a nonpartisan organization that promotes constructive US leadership and engagement in international affairs based on the central role of the Atlantic community in meeting today's global challenges.



Atlantic Council

1030 15th Street, NW, 12th Floor,
Washington, DC 20005

(202) 463-7226, www.AtlanticCouncil.org