Congress of the United States

Washington, DC 20515

June 20, 2025

The Honorable Gene L. Dodaro
Comptroller General of the United States
Government Accountability Office
441 G Street NW
Washington, DC 20548

Mr. Dodaro:

We write to request an investigation of federal law enforcement agencies' use of automated technologies to label individuals as potential threats on the basis of their facial expressions, their body movements, or the content of their speech. We are concerned that such technologies are ineffective as a means of investigating criminal activity, threaten due process and freedom of expression, and pose particular risk to marginalized and vulnerable communities.

The Government Accountability Office (GAO) has been effective in investigating new developments in the federal government's use of surveillance technologies. In 2021, the GAO revealed that the government used facial recognition technology to identify individuals protesting the murder of George Floyd. In 2024, the GAO found serious privacy, civil rights, and effectiveness concerns with police use of biometric identification technologies. Also in 2024, the GAO recommended that the Department of Homeland Security (DHS) assess and mitigate bias risks prior to its component agencies' use of detection, observation, and monitoring technologies.

We have learned that the Department of Justice (DOJ) and DHS are utilizing technologies that make dubious automated inferences about individuals' emotions, attitudes, and intentions. The developers of these technologies claim they can make such determinations on the basis of physical measurements, such as facial expressions, eye movements, or gait, or from content that individuals create and share online, such as text or images. These technologies are based on controversial applications of methods from the artificial intelligence (AI) fields known as affective computing, emotion recognition, sentiment analysis, and deception detection.[1]

For example, in March of this year Axios reported on the "Catch and Revoke" initiative, in which DHS and DOJ are helping the Department of State use AI to scan the social media accounts of tens of thousands of student visa holders and flag some as supposedly supporting terrorist organizations.[2] However, as the Foundation for Individual Rights and Expression commented, AI "cannot be relied on to parse the nuances of expression about complex and contested matters."[3] We fear that AI's inability to make such determinations accurately might actually be the reason the administration is using it in this case. Invoking AI in this way lends

[1] Many researchers in these AI fields have objected to such applications of their research, including applications by law enforcement. For instance, a prominent researcher in the field of automatic emotion recognition (AER) cautions that "AER systems should not claim to determine one's emotional state from [an individual's] utterance, facial expression, gait, and so forth. At best, AER systems capture what one is trying to convey or what is perceived by the listener/viewer, and even there, given the complexity of human expression, they are often inaccurate." See: Saif M. Mohammad, "Ethics Sheet for Automatic Emotion Recognition and Sentiment Analysis", Computational Linguistics, Volume 48, Issue 2 (2022). See also: "Emotion AI researchers say overblown claims give their work a bad name", MIT Technology Review (February 14, 2020).

[2] "Scoop: State Dept. to use AI to revoke visas of foreign students who appear 'pro-Hamas'", Axios (Mar. 6, 2025).

[3] "Rights advocates concerned by reported US plan to use AI to revoke student visas", Reuters (March 6, 2025).

a facade of objectivity to what is in fact a sweeping attempt to punish the expression of views the administration dislikes. In fact, the administration has not presented evidence that the students it has targeted for deportation actually advocated terrorism.[4]

Numerous empirical studies have cast doubt on the reliability of AI methods for inferring individuals' intentions, emotions, or other mental states from external signals such as their facial movements or decontextualized online speech. For example, a review of psychological research on facial expressions concluded that "emotion categories are NOT expressed with facial movements that are sufficiently reliable and specific across contexts, individuals, and cultures to be considered diagnostic displays of any emotional state."[5] Similarly, psychologists have observed "ubiquitous problems in current research into AI-based deception detection" including "the underlying assumption that it is possible to identify a unique cue or combination of cues that is indicative of deception."[6] Some companies market technologies that they claim detect deception with high accuracy, based on physiological activity such as eye movements or changes in voice pitch, claims which either lack independent and replicable evidence[7] or have been contradicted by multiple empirical studies.[8] At the same time, researchers have found evidence suggesting racial, gender, and other demographic biases in the kinds of AI models used for affective computing,[9] lie detection,[10] and sentiment analysis.[11]

It is particularly dangerous to use AI for inferring mental states in law enforcement contexts, where false positives can subject individuals to baseless investigation and detention. Furthermore, since many criminal statutes require proof of intent or other state of mind, using AI in this way could lead prosecutors to bring more severe charges against individuals on the basis of pseudoscientific evidence. This technology is also ripe for deliberate abuse, providing a pretext for government officials to target groups they disfavor.

Unfortunately, this is not the first time the federal government has applied AI to classify individuals as potential security threats. In the last several years, agencies in both DHS and DOJ have contracted with private vendors to use automated technologies that collect and analyze social media posts to make predictions about individuals' attitudes, character, and intentions. For example:

- From 2019 to 2024, U.S. Customs and Border Protection (CBP) used the ONYX AI software from the company Fivecast to analyze online information in order to obtain "insights on potential threats and

[4] "What we know about the foreign college students targeted for deportation", ABC News (April 6, 2025).

[5] Lisa Feldman Barrett, Ralph Adolphs, Stacy Marsella, Aleix M. Martinez, and Seth D. Pollak, "Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements", Psychological Science in the Public Interest, Volume 20, Issue 1 (2019).

[6] Kristina Suchotzki and Matthias Gamer, "Detecting Deception with Artificial Intelligence: Promises and Perils", Trends in Cognitive Sciences, Volume 28, Issue 6 (2024).

[7] "An eye-scanning lie detector is forging a dystopian future", Wired (December 4, 2018). See also: "Lie detector firm lobbies CIA, DOD on automated eye-scanning tech", The Intercept (April 7, 2023).

[8] Brad McCall, "Voice Stress Analysis: Is 'Some Evidence' Sufficient Grounds for Making Legal Determinations?", Barry Law Review, Volume 29, Issue 1 (2024).

[9] Isaac Slaughter, Craig Greenberg, Reva Schwartz, and Aylin Caliskan, "Pre-trained Speech Processing Models Contain Human-Like Biases that Propagate to Speech Emotion Recognition", Findings of the Association for Computational Linguistics: Conference on Empirical Methods in Natural Language Processing (2023).

[10] "Detecting Deception with Artificial Intelligence: Promises and Perils" (see note 6 above).

[11] Svetlana Kiritchenko and Saif Mohammad, "Examining Gender and Race Bias in Two Hundred Sentiment Analysis Systems", Proceedings of the Seventh Joint Conference on Lexical and Computational Semantics (2018).

risks," according to the DHS AI use-case inventory.[12] CBP has shared little information on how it was using ONYX to assess risks to the United States. However, as 404 Media reported in 2023, Fivecast's marketing materials claim their technology can search social media for information about specific individuals, "groups," or "events," including posts related to user-specified ideological movements, and can label the "sentiment and emotion" of posted content.[13]

- The Washington Post reported in 2022 that the FBI signed a five-year contract to use Babel X, an AI-based platform for searching and analyzing social media content.[14] This contract fulfills a request for proposals for systems to search social media based on user location or "demographic information" and conduct "sentiment analysis" on posts to "provide analysis on emotion and likely attitudes" of users and "predictive analytics … that point towards possible actions of a subject or group."[15] VICE reported that CBP also began using Babel X in 2019 to analyze online content in order to identify travelers for enhanced security screening, including U.S. citizens and permanent residents. CBP noted in internal documents that Babel X helps its agents identify "threats to CBP and national security" with capabilities that include filtering posts by hashtags, "events," and "known terms used by bad actors," as well as analyzing the "sentiment" of posts.[16]

- As part of its Extreme Vetting Initiative, U.S. Immigration and Customs Enforcement (ICE) solicited proposals in 2017 from companies for systems that would use AI to analyze social media posts of visa applicants to predict their likelihood of committing crimes or to be "positively contributing member[s] of society." The following year ICE concluded that no existing product was up to the task.[17]

- Since 2020, ICE has paid the contractor Barbaricum to conduct automated searches of social media platforms for posts threatening ICE.[18] In its original request for bids, ICE was vague about how it defined threatening posts, but it specified that the contractor should provide "monitoring and analysis of behavioral and social media sentiment" and regular reports on the "number of negative references to ICE found in social media during monitoring."[19]

In addition to these concerning uses of sentiment analysis for law enforcement purposes, federal agencies have also shown interest in affective computing and deception detection technologies that purportedly infer individuals' mental states from measures of their facial expressions, body language, or physiological activity. In 2011, DHS field-tested its Future Attribute Screening Technology (FAST), which DHS claimed could screen

[12] U.S. Department of Homeland Security, "AI at DHS: A Deep Dive into our Use Case Inventory" (December 16, 2024). Available at: https://www.dhs.gov/archive/news/2024/12/16/ai-dhs-deep-dive-our-use-case-inventory

[13] "The A.I. surveillance tool DHS uses to detect 'sentiment and emotion'", 404 Media (August 24, 2023).

[14] "The FBI is spending millions on social media tracking software", Washington Post (April 5, 2022).

[15] Federal Bureau of Investigation, Notice ID 15F06722R0000005, "Tactical Social Media Exploitation Tool" (December 17, 2021). Available at: https://sam.gov/opp/b8815efda887453eb3fee7b310de9280/view.

[16] "Homeland Security uses AI tool to analyze social media of U.S. citizens and refugees", VICE (May 17, 2023).

[17] "ICE just abandoned its dream of 'extreme vetting' software that could predict whether a foreign visitor would become a terrorist", Washington Post (May 17, 2018).

[18] "ICE wants to know if you're posting negative things about it online", The Intercept (February 11, 2025).

[19] U.S. Immigration and Customs Enforcement, Notice ID 70CMSW20R00000002, "Internet Based Threat Risk

Mitigation and Monitoring Services" (Feb 28, 2020). Available at: https://sam.gov/opp/2f12a1fa2497438c80c4d69b2d81b1b5/view.

travelers at security checkpoints by detecting “deception” and “intent to cause harm” based on “physiological and behavioral cues,” such as travelers’ eye movements, facial expressions, heart rates, and breathing patterns.[20] In 2011-2012, researchers tested a DHS-funded AI lie-detector based on similar measurements, called the Automated Virtual Agent for Truth Assessment in Real Time (AVATAR), at a border checkpoint.[21]

Private companies also market similar deception detection products to law enforcement agencies, and count federal agencies among their customers. Converus sells a system called EyeDetect, which it claims can spot liars with high accuracy by measuring eye movements and pupil dilation. The State Department’s Bureau of International Narcotics Control and Law Enforcement Affairs (INL) currently has a contract with Converus for EyeDetect equipment.[22] In addition, the Defense Department’s Defense Counterintelligence and Security Agency is funding research at the US-Mexico border to test EyeDetect’s usefulness for law enforcement.[23] The CEO of Converus claims to have also demonstrated EyeDetect to the FBI and DHS.[24]

Similarly, a company called NITV Federal Services sells a Computer Voice Stress Analyzer (CVSA). NITV claims CVSA uses machine learning to detect deception from changes in voice pitch, and sells this product to law enforcement and government agencies, including the Department of the Interior.[25]

To aid in our evaluation of the potential threats these technologies pose to the effectiveness of law enforcement investigations, as well as to due process, freedom of expression, and civil rights, we request that GAO produce a report that answers the following questions about how DOJ and DHS are using AI technologies to infer people’s emotions, attitudes, or intentions:

- To what extent are the Department of Justice and the Department of Homeland Security using such AI technologies for law enforcement purposes? In particular:
    - Approximately how many people have been the subject of an automated analysis conducted by DOJ or DHS personnel using these technologies?
    - What kinds of law enforcement actions have been guided by DOJ and DHS personnel’s use of these technologies?
- How have DOJ and DHS acquired these AI technologies?
- What tests of these technologies did DOJ and DHS conduct or review before using them for law enforcement purposes?
- How have DOJ and DHS assessed the costs and benefits of using these technologies?
- What DOJ and DHS policies govern the uses of these AI technologies and what guidance or training do they provide to personnel in order to prevent violations of due process, freedom of expression, equal protection, and other constitutional rights?
- How do DOJ and DHS ensure the AI technologies are used in accordance with agency policies?

[20] “Why Homeland Security’s pre-crime prevention technology is a terrible idea”, Slate (April 18, 2012).

[21] “Lie-detecting computer kiosks equipped with artificial intelligence look like the future of border security”, CNBC (May 15, 2018).

[22] See: Award ID 191NLE24P0082 at https://www.usaspending.gov.

[23] “Bush School Team Awarded Project to Study Effectiveness of Lie-Detection System That Tracks Eye Behavior”, Texas A&M University Bush School of Government and Public Service (February 14, 2024). Available at: https://bush.tamu.edu/news/bush-school-team-awarded-project-to-study-effectiveness-of-lie-detection-system-that-tracks-eye-behavior

[24] “The eyes don’t lie, and new technology shows why”, Policing Matters Podcast, Episode 329 (May 25, 2022).

[25] See: Award ID 140A1625P0017 at https://www.usaspending.gov.

Thank you for your attention to this matter.

Sincerely,

Ron Wyden

Ron Wyden
United States Senator
Ranking Member, Committee on Finance

Edward J. Markey

Edward J. Markey
United States Senator

Chris Van Hollen
Ranking Member
Subcommittee on Commerce, Justice, Science, and Related Agencies

Peter Welch

Peter Welch
United States Senator

Pramila Jayapal
Ranking Member
Subcommittee on Immigration Integrity, Security, and Enforcement

Bennie G. Thompson

Bennie G. Thompson
Ranking Member, Committee on Homeland Security

Cory A. Booker
United States Senator