Congressional Research Service
Informing the legislative debate since 1914

Facial Recognition Technology: Definitions, Applications, and Policy Considerations for Congress

May 4, 2026

Congressional Research Service
https://crsreports.congress.gov
R48935

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

SUMMARY

R48935

May 4, 2026

Dominique T. Greene-Sanders
Analyst in Science and Technology Policy

Facial Recognition Technology: Definitions, Applications, and Policy Considerations for Congress

Facial recognition technology (FRT) is a type of biometric technology designed to identify or verify an individual by analyzing unique and measurable facial features. FRT has received attention from policymakers and the public, in large part because of technical advances and use by both public and private sector entities. FRT usage has the potential to optimize performance, enhance security, and increase the speed of tasks that were once handled by humans (e.g., identity verification in airports). The use of FRT has raised issues regarding data privacy and disclosure of its use, as well as bias and accuracy—particularly across different demographic groups.

There is no universally accepted definition of FRT, and disagreement persists among technology developers, policymakers, and academics regarding what the term includes when used in various contexts. Legislation and guidelines have offered differing definitions of FRT, ranging from narrow ones focused on verification and identification to broader interpretations that include emotion detection, age estimation, and facial characteristic classifications. Different definitions may affect which technologies are categorized as FRT.

FRT is employed across a wide range of sectors, including the military, law enforcement, financial services, public health, and education, as well as in activities such as employment decisions and immigration enforcement. FRT usage offers several potential benefits, such as increased security, efficiency, and convenience. Additionally, FRT usage raises concerns, for example, whether FRT systems are designed and deployed in ways that avoid or mitigate bias and are transparent and accurate—particularly across different demographic groups. FRT applications in three particular sectors—transportation and airport security, housing, and law enforcement—have garnered specific interest from the public, Congress, and industry, based on perceptions of the frequency of FRT's use and its potential risks and benefits.

Some state and local governments have passed laws to prohibit or restrict FRT use, especially by law enforcement. As Congress debates the use of FRT across various sectors, it may consider an approach that balances support for innovation and the beneficial uses of FRT while minimizing potential risks. In particular, Congress may consider how FRT is defined in order to avoid inadvertent restriction of narrower identity verification uses, such as personal smartphone access. Considerations for Congress might also include whether existing mechanisms are sufficient for determining accountability regarding FRT use by federal agencies and others. Finally, Congress may also consider requirements for disclosure of FRT use and for testing and validation of FRT systems, potential ways to require FRT system evaluations for federal use, and mechanisms to incentivize FRT system evaluations for commercial use.

Contents

Contacts

Introduction

Facial recognition technology (FRT) uses algorithms to compare identity information by examining the digitally perceived placement of an individual's facial features. FRT is a specific type of *biometric technology*, which is a broader category encompassing methods of identifying individuals on the basis of biological or behavioral characteristics (e.g., fingerprints and iris scans).[1] Though development of FRT began over 40 years ago, it has received specific attention from policymakers and the public over the past decade or so, in large part because of technical advances, like the growth of artificial intelligence (AI), and use by public and private sector entities. Applications of FRT have expanded across sectors such as housing, transportation, finance, and education. The growth in FRT uses presents opportunities and challenges for users and policymakers alike and raises questions on how to define and whether to regulate FRT in order to monitor its implementation and effects. Potential benefits relating to the widespread use of FRT include enhancing public safety and user convenience (e.g., accessing devices), reducing fraud, and improving operational efficiencies. In contrast, widespread use of FRT raises sociotechnical[2] concerns, for example, whether FRT systems are designed and deployed in ways that avoid or mitigate bias and are transparent and accurate—particularly across different demographic groups.

Debate is further complicated by the lack of a clear or consistent definition of FRT, leading stakeholders to reference different types or capabilities of the technology—which may impede Congress's ability to craft clear, targeted, and enforceable legislation.

This report provides a brief overview of FRT and discusses varying definitions for the technology. The report includes an overview of some current applications of FRT in various sectors, including housing, law enforcement, and transportation. It also discusses selected policy considerations for Congress.

FRT Overview

FRT has evolved since its initial development in the 1960s. Early research focused on mapping facial features manually, with researchers pioneering methods for using computers to recognize up to 10 different faces.[3] By the 1990s, automated facial recognition had progressed as a result of improved computational power and technical advances in enabling machines to interpret and understand visual information.

Progress accelerated in the 2000s with the development of standardized facial image datasets and algorithm benchmarks for detection, image analysis, and recognition. These technological advances were possible in part because of efforts by the U.S. government, particularly the National Institute of Standards and Technology (NIST).[4] By the 2010s, widespread commercial

[1] U.S. Department of Homeland Security (DHS) et al., *Biometric Technology Report*, December 26, 2024, https://www.dhs.gov/sites/default/files/2024-12/24_1230_st_13e-Final-Report-2024-12-26.pdf.

[2] *Sociotechnical* refers to the interdependent relationship between technical systems and societal factors in which optimizing one part requires considering the other. See, for example, Brian J. Chen and Jacob Metcalf, "Explainer: A Sociotechnical Approach to AI Policy," Data & Society, May 2024, https://datasociety.net/wp-content/uploads/2024/05/DS_Sociotechnical-Approach_to_AI_Policy.pdf.

[3] Mark Andrejevic and Neil Selwyn, *Facial Recognition* (Polity, 2022) (hereinafter Andrejevic and Selwyn, *Facial Recognition*).

[4] Testimony of Director of the Information Technology Laboratory, National Institute of Standards and Technology (continued...)

adoption began, as facial recognition became integrated into both the private and public sectors to promote security, speed, and streamlined convenience. Private sector applications include smartphone unlocking, photo tagging on social media platforms, and retail analytics.[5] Entities may use FRT for digital access and physical security. For example, the General Services Administration (GSA) and Social Security Administration (SSA) reported testing FRT systems' ability to control access to certain government websites (e.g., GSA's login.gov) by having the system "compare two images—a government photo identification and a live image of the individual—to verify the identity of an individual attempting to apply for an account."[6] Other examples of potential public sector uses include federal, state, and local law enforcement activities;[7] airport security; and surveillance.[8] As the use of FRT has expanded, public awareness and scrutiny of the technology has grown, prompting debates regarding its regulation and use.[9]

How Does FRT Work?

FRT systems can involve various technologies and processes. Although the design and terminology can vary, most FRT algorithms follow a similar sequence of operations that allow machines to detect, analyze, and compare human faces. These operations are generally categorized into three parts:

1. *Detection:* the foundational function in most facial recognition processes, this first step identifies whether an image or video contains a human face.
2. *Feature extraction:* this step involves extracting distinct facial features from an image to create a mathematical representation of that face (sometimes referred to as a "template").
3. *Facial comparison:* this function attempts to match a template from the detected face to one or more known faces, producing a "similarity score" (sometimes called a "match score"), which is a numerical value that shows how closely two faces match based on their features.[10]

(NIST), Charles H. Romine in U.S. Congress, House Committee on Homeland Security, *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies, Part II*, hearings, 116th Cong., 2nd sess., February 6, 2020, H.Hrg. 116-60, https://www.govinfo.gov/content/pkg/CHRG-116hhrg41450/pdf/CHRG-116hhrg41450.pdf (hereinafter Romine, Testimony in H.Hrg. 116-60).

[5] Andrejevic and Selwyn, *Facial Recognition*.

[6] U.S. Government Accountability Office (GAO), *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, GAO-21-526, August 24, 2021, p. 12, https://www.gao.gov/products/gao-21-526.

[7] U.S. Congress, House Committee on Oversight and Government Reform, *Law Enforcement's Use of Facial Recognition Technology*, 115th Cong., 1st sess., March 22, 2017, H.Hrg. 115-52. See also Christopher Jones, "Law Enforcement Use of Facial Recognition: Bias, Disparate Impacts to People of Color, and the Need for Federal Legislation," *North Carolina Journal of Law and Technology*, vol. 22, no. 4 (May 1, 2021), pp. 777-815.

[8] For more information on facial recognition technology (FRT) in global security, see CRS In Focus IF11783, *Biometric Technologies and Global Security*, by Kelley M. Sayler.

[9] U.S. Commission on Civil Rights, "U.S. Commission on Civil Rights Releases Report: The Civil Rights Implications of the Federal Use of Facial Recognition Technology," press release, September 19, 2024, https://www.usccr.gov/news/2024/us-commission-civil-rights-releases-report-civil-rights-implications-federal-use-facial (hereinafter U.S. Commission on Civil Rights, "The Civil Rights Implications of the Federal Use of Facial Recognition Technology"). See also Josh Blatt, "Advances in Facial Recognition Technology Have Outpaced Laws, Regulations; New Report Recommends Federal Government Take Action on Privacy, Equity, and Civil Liberties Concerns," National Academies of Sciences, Engineering, and Medicine (NASEM), press release, January 17, 2024, https://www.nationalacademies.org/news/2024/01/advances-in-facial-recognition-technology-have-outpaced-laws-regulations-new-report-recommends-federal-government-take-action-on-privacy-equity-and-civil-liberties-concerns.

[10] NASEM, *Facial Recognition Technology: Current Capabilities, Future Prospects, and Governance* (National Academies Press, 2024), p. 33 (hereinafter NASEM, *Facial Recognition Technology*).

Generally, facial comparison is a means of identity recognition through either

- *verification* (one-to-one matching), which confirms whether a face in a new image matches a specific known face and is often used for authentication (e.g., unlocking phones or verifying identity on government-issued IDs), or
- *identification* (one-to-many matching), which searches a database to determine whether the detected face corresponds to any known individual and is often used for investigative purposes.[11]

These components are not always strictly delineated. Some systems may have additional steps not listed above, or they may combine steps, as described below. The specifics may differ depending on intended environment, use case, and available data.

Defining FRT

Despite its prominence, disagreement persists among technology developers, policymakers, and academics regarding how to define FRT and what the term includes when used in various contexts.

Technology experts acknowledge that "there is no one standard system design for facial recognition systems. Not only do organizations build their systems differently, and for different environments, but they also use different terms to describe how their systems work."[12] This lack of consistency in defining and characterizing FRT systems can manifest in various ways. For example, reports on FRT systems may use the term *face* or *facial*, though their descriptions appear to be interchangeable. Additionally, terms such as *facial detection* and *facial analysis*[13] may refer to components of FRT systems[14] or to distinct systems used for non-identifying categorization purposes. For example, a 2021 Government Accountability Office (GAO) report refers to *facial detection* and *facial analysis* as being related to but distinct from *facial recognition*—matching a face for identification. As described in that report, *facial detection* systems essentially stop at the detection step, determining whether a digital image contains a face, for example, to quantify how many people move through an area without being categorized or identified. Facial analysis, or facial classification/characterization, systems analyze a facial image to estimate or classify personal characteristics, such as age, race, or sex, but do not identify individuals. These systems might also track facial features or movement to recognize expressions or eye movement, among other analyses. However, GAO, for the purposes of its report, defines FRT "to include facial recognition, facial detection, or facial analysis technologies."[15] This inclusive definition provides an example of the indistinctness that can exist when determining the definition and scope of FRT.

While some analyses may group technologies under the term *FRT* for simplicity, entities may not accurately describe the capability of FRT-marketed systems. For example, facial analysis tools are

[11] Romine, Testimony in H.Hrg. 116-60.

[12] Partnership on AI, *Understanding Facial Recognition Systems*, February 19, 2020, p. 3, https://old.partnershiponai.org/wp-content/uploads/2020/02/Understanding-Facial-Recognition-Paper_final.pdf.

[13] Also referred to as *face detection* and *face analysis*.

[14] For example, facial detection capabilities and facial analysis capabilities were considered part of Microsoft's FRT system. Microsoft retired and/or limited "facial analysis capabilities that purport to infer emotional states and identity attributes such as gender, age, smile, facial hair, hair, and makeup." Sarah Bird, "Responsible AI Investments and Safeguards for Facial Recognition," *Microsoft Azure* (blog), Microsoft, June 21, 2022, https://azure.microsoft.com/en-us/blog/responsible-ai-investments-and-safeguards-for-facial-recognition/.

[15] GAO, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, GAO-21-526, p. 6.

sometimes marketed as facial recognition tools, even if they do not perform identity matching.[16] Similarly, systems performing identity verification may also estimate non-identifying attributes—age, gender, and emotional state—during processing should the same features help determine similarity in identity.[17] In other contexts, such as in medical diagnosis or behavioral research, the term *facial recognition* may operate independently from identity recognition.[18] In addition, the Transportation Security Administration (TSA) refers to its one-to-one verification FRT as *facial comparison technology*.[19] The definitional differences in FRT-related terms is further compounded by overlapping functionalities in modern systems and the integration of tools that may perform both types of tasks simultaneously.[20]

Congressional proposals in the 119th Congress have offered differing definitions for FRT, as highlighted in the examples below.

- The No Biometric Barriers to Housing Act of 2025 (H.R. 3060, 119th Congress) would define FRT broadly to include systems that log "characteristics of an individual's face, head, or body to infer emotion, associations, activities, or the location of an individual."
- In contrast, H.R. 3782 (119th Congress), a bill "to prohibit the Federal Government from using facial recognition technology as a means of identity verification, and for other purposes," would define FRT more narrowly as "a contemporary security system that automatically identifies and verifies the identity of an individual from a digital image or video frame."

Federal agencies have also used different terms when defining the scope of its applications. For example, in 2000, NIST began a Face Recognition Vendor Test (FRVT) program, which assessed the performance of facial recognition algorithms broadly.[21] In response to the inclusion of non-identifying analytical tools not initially distinguished or captured within the FRVT program, NIST split the program in 2023 into two distinct evaluation tracks:

- The *Face Recognition Technology Evaluation (FRTE)* track focuses on the evaluation of identification and verification systems.
- The *Face Analysis Technology Evaluation (FATE)* track focuses on evaluating systems that process and analyze images purposes such as for age estimation, authenticity, and overall quality.[22]

Nongovernment entities also use FRT and FRT-related terms differently. One analysis from the Ada Lovelace Institute, a European independent research organization focused on data technology and AI, states that FRT "is a complex area, which means the risk of

[16] Andrejevic and Selwyn, *Facial Recognition*.

[17] Samuel Wehrli et al., "Bias, Awareness, and Ignorance in Deep-Learning-Based Face Recognition," *AI and Ethics*, vol. 2, no. 3 (2022), pp. 509-522.

[18] Vera Lucia Raposo, "Facial Recognition AI Technology in Healthcare and the Law," in *Research Handbook on Health, AI and the Law* (Edward Elgar, 2024).

[19] U.S. Transportation Security Administration (TSA), "Facial Comparison Technology," accessed November 24, 2025, https://www.tsa.gov/news/press/factsheets/facial-comparison-technology.

[20] Mohammad Rasool Izadi, "Feature Level Fusion from Facial Attributes for Face Recognition," *arXiv*, August 11, 2021, https://arxiv.org/pdf/1909.13126. See also Hao Zheng et al., "A Multi-Task Model for Simultaneous Face Identification and Facial Expression Recognition," *Neurocomputing*, vol. 171 (January 2016), pp. 515-523.

[21] Romine, Testimony in H.Hrg. 116-60.

[22] NIST, "Face Technology Evaluations - FRTE/FATE," April 22, 2025, https://www.nist.gov/programs-projects/face-technology-evaluations-frtefate.

misunderstandings is high."[23] The Center for Strategic & International Studies (CSIS) distinguishes facial characterization and classification technology from FRT, asserting that the purpose of FRT is "to compare two different faces."[24] Amazon Web Services describes FRT as "a way of identifying or confirming the identity of an individual using an image of their face."[25] Publicly available definitions and descriptions vary, as does their adoption by users, which may make it difficult for those to whom the technologies are applied to understand which specific applications of FRT are included.

Selected Applications of FRT and Associated Sociotechnical Concerns

FRT is applied across a wide range of sectors, including the military, law enforcement, financial services, public health, and education, as well as in activities such as employment decisions and immigration enforcement. In many cases, this application is part of efforts to enhance the security, efficiency, and speed of identity verification. The ways, and the extent to which, FRT is used across these sectors varies and may complement other biometric technologies (e.g., fingerprinting, iris scans). Army researchers have developed FRT techniques that can identify individuals in low-light or nighttime conditions through thermal imaging that "produces a visible face."[26] The Department of Health and Human Services is reportedly using FRT, among other things, to monitor some facilities for specific individuals and to support criminal investigations.[27] The health care industry may use biometric technologies, such as FRT, to verify the identity of patients and health care staff.[28]

These examples demonstrate several potential benefits of FRT, such as increased security, efficiency, and convenience. The use of FRT also raises sociotechnical concerns related to how it is developed and applied.

Selected Sociotechnical Concerns for FRT

This section of the report highlights selected sociotechnical concerns relating to FRT.

Accuracy, Bias, and Explainability

The accuracy and explainability of FRT systems—as well as the assessment and mitigation of any bias associated with their development and use—are key areas of interest for stakeholders. *Accuracy* refers to whether systems correctly match or identify individuals, particularly in

[23] Jenny Brennan, "Facial Recognition: Defining Terms to Clarify Challenges," Ada Lovelace Institute (blog), November 13, 2019, https://www.adalovelaceinstitute.org/blog/facial-recognition-defining-terms-to-clarify-challenges/.

[24] Center for Strategic & International Studies (CSIS), "How Does Facial Recognition Work?," June 10, 2021, https://www.csis.org/analysis/how-does-facial-recognition-work.

[25] Amazon, "What Is Facial Recognition?," accessed November 28, 2025, https://aws.amazon.com/what-is/facial-recognition/.

[26] Army Research Laboratory Public Affairs, "Army Develops Face Recognition Technology that Works in the Dark," U.S. Army, April 18, 2018, https://www.army.mil/article/203901/army_develops_face_recognition_technology_that_works_in_the_dark. For more information on FRT in the Armed Forces, see CRS In Focus IF11783, *Biometric Technologies and Global Security*, by Kelley M. Sayler.

[27] GAO, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies*, GAO-21-526, p. 13.

[28] GAO, *Biometric Identification Technologies: Considerations to Address Information Gaps and Other Stakeholder Concerns*, GAO-24-106293, April 22, 2024, p. 10, https://www.gao.gov/assets/gao-24-106293.pdf (hereinafter GAO, *Biometric Identification Technologies*, GAO-24-106293).

contexts where errors may have legal, social, or economic consequences. Questions regarding *bias*[29] are commonly raised in instances where some FRT systems perform differently across demographic groups, though numerous different types of bias may arise in FRT systems, as with systems that rely on AI more broadly.[30] *Explainability* is also discussed in this same context as the operator's ability to understand how an FRT system arrives at a result and how that may affect assessments of reliability, fairness, and oversight.[31] These questions are usually linked to questions on how systems are developed and evaluated.

While the overall technical accuracy of many commercial FRT systems has increased over the past decade, researchers have documented that FRT may be less accurate for certain demographic groups based on such factors as skin tone, gender, and age.[32] Accuracy can be assessed by looking at the number of accurate results—true positive results (i.e., an accurate match) or true negative results (i.e., an accurate non-match)—and the number of inaccurate results, which consist of two main types of errors: *false positive* and *false negative*. A false positive result occurs when an FRT system reports that two images are a match when they are not, and a false negative result occurs when a system reports that two images are not a match when they actually are.[33] Errors may also occur because of technical failures relating to the facial image not being captured or "the algorithm failing to find or extract usable features from an image" as a result of dim lighting, poor image quality, or other factors.[34] Further, some reporting has noted that such technical factors for higher error rates may affect certain demographic groups disproportionately,[35] which may be due to multiple technical and human factors (e.g., lack of diverse representation in training data). Such instances may place individuals from those groups at higher risk of being misidentified or not identified at all, which may have unintended consequences, such as being fired from a job or falsely detained.[36]

Statistical (or computational) biases in FRT systems, such as those arising from factors such as a lack of diversity in the images on which the systems were trained, can also contribute to higher

[29] Bias exists in many forms, and definitions vary. NIST identifies three main categories of artificial intelligence (AI) bias: systemic, computational and statistical, and human cognitive. Systemic bias comes from procedures and practices that result in certain demographic groups being favored while others are disadvantaged (e.g., sexism, ableism, and institutional racism). Computational and statistical bias comes from nonrepresentative samples causing systematic errors. Human cognitive biases relate to how the purpose and functions of an AI system or AI system information are perceived by humans. Schwartz et al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, NIST Special Publication 1270, pp. 6-9. See also NIST, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, January 2023, https://doi.org/10.6028/NIST.AI.100-1. For more information on bias in AI, see CRS Report R46795, *Artificial Intelligence: Background, Selected Issues, and Policy Considerations*, by Laurie Harris.

[30] See, for example, Reva Schwartz et al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, NIST Special Publication 1270, March 15, 2022, pp. 6-9, https://nvlpubs.nist.gov/NISTpubs/SpecialPublications/NIST.SP.1270.pdf (hereinafter Schwartz et al., *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, NIST Special Publication 1270).

[31] For more information on explainable AI, see CRS Report R46795, *Artificial Intelligence: Background, Selected Issues, and Policy Considerations*, by Laurie Harris. See also P. Jonathon Phillips et al., *Four Principles of Explainable Artificial Intelligence*, NIST Interagency Report 8312, September 2021, https://nvlpubs.nist.gov/nistpubs/ir/2021/nist.ir.8312.pdf.

[32] Ketan Kotwal and Sébastien Marcel, "Review of Demographic Bias in Face Recognition," *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 8, no. 1 (January 2026), pp. 20-45. See also GAO, *Biometric Identification Technologies*, GAO-24-106293, p. 19.

[33] GAO, *Biometric Identification Technologies*, GAO-24-106293, p. 11.

[34] NASEM, *Facial Recognition Technology*, p. 48.

[35] GAO, *Rental Housing: Use and Federal Oversight of Property Technology*, GAO-25-107196, July 10, 2025, p. 14, https://www.gao.gov/products/GAO-25-107196 (hereinafter GAO, *Rental Housing*, GAO-25-107196).

[36] Inioluwa Deboral Raji, "The Anatomy of AI Audits: Form, Process, and Consequences," in *The Oxford Handbook of AI Governance*, ed. Justin B. Bullock et al. (Oxford University Press, 2022), p. 508.

error rates. According to GAO, biometrics research is mostly performed by the private sector and focuses primarily on "improving overall accuracy and efficiency" rather than "reducing error rate differences between demographic groups."[37] For example, some FRT has been shown to have significant gender and skin color classification bias; one 2023 Department of Homeland Security (DHS)-sponsored study testing demographic effects across 158 FRT systems using regression modeling at a DHS test facility reported that 99% of models had similarity scores that were higher for lighter-skinned participants,[38] and 74% of models had similarity scores that were lower for women compared with historic images from prior tests. The study found that conclusions from previous 2018-2021 studies "remain consistent" with reporting demographics disclosed by participants (e.g., gender and use of eye ware) and skin lightness affects the system's confidence in identifying the person.[39] According to GAO, NIST's original FRVT program found that FRT usually "performs better on lighter-skinned men than it does on darker-skinned women, and does not perform as well on children and elderly adults as it does on younger adults."[40] Similarly, another 2025 DHS-sponsored study at the same DHS test facility found that some contemporary FRT systems that rely on older, nonproprietary methods detected the faces of 99.7% of lighter-skinned subjects and approximately 76% of darker-skinned subjects in certain real-world testing scenarios—demonstrating a gap in performance under real-world scenario testing.[41]

Accountability, Transparency, Privacy, and Data Security

Considerations of accountability and transparency also often touch on topics of privacy and data security. *Accountability* refers to how responsibility for FRT deployment—including for potential errors, misuse, and unintended outcomes—is distributed among developers, vendors, and entities that use the technology. *Transparency* relates to the degree to which FRT use is disclosed to policymakers, oversight bodies, and/or the public. This could include information such as whether individuals are informed about the purpose and presence of FRT use, how their data are handled, and how information on FRT use is disclosed. *Privacy* considerations address how FRT use affects consent, expectations of anonymity, and an individual's control over personal information. According to a 2025 survey by ExpressVPN, 44% of employees did not know whether their employer uses biometric surveillance methods.[42] Regarding *data security*, descriptions of FRT use often address how facial data are collected, stored, shared and protected, as well as how long they should or would be retained.

With insights from federal, industry, and nonprofit AI experts, GAO created an "AI accountability framework" in 2021 consisting of four principles to address "responsible AI use by federal agencies and other entities involved in the design, development, deployment, and continuous

[37] GAO, *Biometric Identification Technologies*, GAO-24-106293, p. 21.

[38] Cynthia M. Cook et al., "Demographic Effects Across 158 Facial Recognition Systems," DHS, August 2023, p. 10, https://www.dhs.gov/sites/default/files/2023-09/23_0926_st_demographic_effects_across_158_facial_recognition_systems.pdf (hereinafter Cook, "Demographic Effects Across 158 Facial Recognition Systems").

[39] Cook, "Demographic Effects Across 158 Facial Recognition Systems," p. 1.

[40] GAO, *Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities*, GAO-21-519SP, June 30, 2021, p. 52, https://www.gao.gov/assets/gao-21-519sp.pdf (hereinafter GAO, *Artificial Intelligence*, GAO-21-519SP).

[41] Cynthia M. Cook et al., "Performance Differentials in Deployed Biometric Systems Caused by Open-Source Face Detectors," in *FAccT: Proceedings of the 2025 Association of Computing Machinery Conference on Fairness, Accountability and Transparency* (June 23, 2025), pp. 2630-2639.

[42] ExpressVPN, "U.S. Survey: 1 in 6 Workers Would Quit Over Workplace Surveillance as Monitoring Increases," June 2, 2025, https://www.expressvpn.com/blog/workplace-surveillance-trends-us/?srsltid=AfmBOore4yYJcRbd4G2cwIkGhKaxDH06W43oZcpZw3Z3GQ4LZb0hIE3G.

monitoring of AI systems."[43] The AI accountability framework identifies key accountability practices based on four principles—governance, data, performance, and monitoring—to promote the responsible use of AI by federal agencies and other entities. The governance principle consists of nine key practices to promote accountability through establishing processes to manage, operate, and oversee the implementation of AI systems. Under the governance principle, one key practice refers to defining clear roles with corresponding responsibilities and designating authority "for the AI system to ensure effective operations, timely corrections, and sustained oversight."[44] Another practice is for organizations to promote transparency by granting external stakeholders access to AI system information relating to design, operations, and restrictions.[45] This framework could be directly applied to modern FRT systems that use AI models.[46]

Applications of FRT in Selected Sectors

This section of the report highlights FRT applications in three sectors: transportation and airport security, housing, and law enforcement. FRT use in these sectors have garnered interest from the public, Congress, and industry, based on perceptions of the frequency of its use and its potential risks and benefits.

Transportation and Airport Security[47]

FRT usage in the transportation sector occurs across different transportation modes. It reportedly includes cameras to identify drivers and monitoring systems to analyze eye movements of commercial truck drivers, train operators, and air traffic controllers for signs of distraction or fatigue.[48] FRT use in the air travel context has been advanced, in part, by federal policies and regulations. Biometric technologies in airports, including FRT, are used by federal and nonfederal entities to facilitate airport operations, access control, commercial services, and risk management.[49] These technologies are designed to enhance security effectiveness and streamline passenger experiences by automating passenger screening processes.[50] For example, the Traveler Verification Service (TVS), a partnership between the federal agencies and private airlines, airports, and other entities, uses a facial recognition matching technology (one-to-many identification) to verify travelers' identities by capturing a live photo and comparing it with existing images in a database (e.g., passport photos).[51] Since 2021, TSA has expanded FRT pilot programs in airports—such as TSA PreCheck's Touchless ID—to enhance security by allowing

[43] GAO, *Artificial Intelligence*, GAO-21-519SP, highlights page.

[44] GAO, *Artificial Intelligence*, GAO-21-519SP, p. 5.

[45] GAO, *Biometric Identification Technologies*, GAO-24-106293, p. 47.

[46] NASEM, *Facial Recognition Technology*, p. 19.

[47] For more information on FRT in transportation, see CRS Report R48543, *Transportation Security: Background and Issues for the 119th Congress*, coordinated by Bart Elias. See also CRS Report R47541, *Immigration: The U.S. Entry-Exit System*, by Abigail F. Kolker.

[48] Byron Tau and Garance Burke, "Border Patrol Is Monitoring US Drivers and Detaining Those with 'Suspicious' Travel Patterns," Associated Press, November 20, 2025, https://apnews.com/article/immigration-border-patrol-surveillance-drivers-ice-trump-9f5d05469ce8c629d6fecf32d32098cd.

[49] NASEM, *Airport Biometrics: A Primer* (National Academies Press, 2021), p. 10 (hereinafter NASEM, *Airport Biometrics: A Primer*).

[50] TSA, "Biometrics Technology," https://www.tsa.gov/biometrics-technology.

[51] The traveler would need to be enrolled in TSA PreCheck and/or Customs and Border Protection (CBP) Global Entry for one-to-many identification. TSA also offers optional FRT one-to-one verification that involves taking a picture of the traveler and comparing it with identity documentation (e.g., passport or driver's license). TSA, "Biometrics Technology," https://www.tsa.gov/biometrics-technology.

enrolled travelers to use dedicated lanes using FRT applications for identity verification.[52] Additionally, TSA PreCheck's Touchless ID also uses the TVS system for customer conveniences, such as a touchless "curb-to-gate" experience, where enrolled travelers with participating airlines can opt in to have FRT applications expedite the luggage check-in and boarding processes.[53]

FRT applications in airport security have raised questions regarding accountability, data security, consumer privacy, and transparency. These questions arise, in part, because the responsibility for a system's outcomes is spread among several different entities, which may include airlines, governmental agencies, and other third parties and individuals.[54] For example, DHS states that in sharing biometric data across agencies, "federal, state[,] local, tribal, and territorial governments—along with international partners—all play a role in the continuum to capture, compare, store, share, analyze, and decide/act on biometric information (such as fingerprints, iris scans, and face images)."[55] TSA states that passengers can opt out of FRT without delays or additional screening; however, some advocacy groups assert that the process for opting out may not be uniformly applied or explained with sufficient clarity for passengers to do so.[56]

Similarly, questions reportedly have arisen regarding how the data are collected, who has access to them, and what happens if a data breach occurs.[57] For example, a 2019 Customs and Border Protection (CBP) biometric pilot had a data breach that "compromised approximately 184,000 traveler images," at least 19 of which "were posted to the dark web."[58] Some privacy advocates cautioned that personal data may be misused, collected, or stored without consent and that legal and security protections may be inadequate to safeguard against these risks.[59]

Housing

FRT reportedly has been adopted by certain landlords, property management companies, and developers for a variety of purposes, such as seeking to enhance tenant security for controlled building access[60] and surveillance.[61] It may be used in both private market housing and in

[52] TSA, "TSA PreCheck Touchless ID," https://www.tsa.gov/touchless-id.

[53] TSA, "TSA PreCheck Touchless ID," https://www.tsa.gov/biometrics-technology/evaluating-facial-identification-technology. See Delta News Hub, "Delta Launches First Domestic Digital Identity Test in U.S., Providing Touchless Curb-to-Gate Experience," January 29, 2021, https://pro.delta.com/content/agency/us/en/news/news-archive/2021/january-2021/delta-launches-first-domestic-digital-identity-test-in-u-s—pro.html. See also Delta News Hub, "Delta's First-Ever Dedicated TSA Precheck Lobby, Bag Drop," accessed December 22, 2025, https://news.delta.com/sites/default/files/2021-10/media_fact_sheet_tsa_precheck.pdf. See also CBP, "Biometrics Environments: Airports," November 13, 2025, https://www.cbp.gov/travel/biometrics/environments/airports.

[54] NASEM, *Airport Biometrics: A Primer*, p. 40. See also GAO, *Artificial Intelligence*, GAO-21-519SP, p. 32.

[55] DHS, "Biometrics," August 28, 2025, https://www.dhs.gov/biometrics.

[56] Shira Ovide, "How to Opt Out of Facial Recognition at the Airport," *Washington Post*, July 29, 2025, https://www.washingtonpost.com/technology/2025/07/29/airport-facial-recognition-scan-opt-out/.

[57] Rebecca Santana, "Senators Want Limits on TSA Use of Facial Recognition Technology for Airport Screening," *PBS News*, May 2, 2024, https://www.pbs.org/newshour/politics/senators-want-limits-on-tsa-use-of-facial-recognition-technology-for-airport-screening.

[58] DHS, Office of Inspector General, *Review of CBP's Major Cybersecurity Incident During a 2019 Biometric Pilot*, OIG-20-71, September 21, 2020, p. 6, https://www.oig.dhs.gov/sites/default/files/assets/2020-09/OIG-20-71-Sep20.pdf.

[59] NASEM, *Airport Biometrics: A Primer*, p. 44.

[60] GAO, *Rental Housing*, GAO-25-107196, p. 8.

[61] Douglas MacMillan, "Eyes on the Poor: Cameras, Facial Recognition Watch Over Public Housing," *Washington Post*, May 16, 2023, https://www.washingtonpost.com/business/2023/05/16/surveillance-cameras-public-housing/ (hereinafter MacMillan, "Eyes on the Poor").

federally subsidized housing, including public housing.[62] These systems may replace or accompany physical keys, fobs, or pin codes with a biometric verification to access building entrances[63] and elevators,[64] as well as to monitor shared spaces such as hallways and mailrooms.[65] According to GAO, FRT systems usually operate by capturing the facial images of authorized individuals, using the algorithms to authenticate and grant access to individuals at entry points. For example, FRT-enabled security cameras may identify residents, approved guests, and authorized personnel (maintenance and staff) to grant building access.[66]

Several organizations have argued that misuse of FRT for monitoring people's behavior and misidentifications could exacerbate issues of marginalized individuals being disproportionately negatively affected by this technology.[67] For example, GAO reported that advocacy groups "expressed concerns" regarding individuals from certain demographic groups (e.g., Black women) having higher error rates when FRT was used for identification and verification purposes, potentially resulting in "frequent access denials for some individuals."[68] According to the National Academies of Sciences, Engineering, and Medicine (NASEM), FRT might also lead to unrecognized family members being denied access to the premises, and video footage has been "used to identify, punish, and evict public housing residents, sometimes for minor violations of housing rules."[69] Such events may be perceived as surveilling and dictating tenants' social circles, which affects the autonomy and privacy of both tenants and their guests.

Additionally, housing providers could be subject to legal liability under antidiscrimination laws, such as the federal Fair Housing Act (FHA). The FHA prohibits discrimination on the basis of race, color, religion, sex, disability, familial status, and national origin in the sale or rental of housing, housing financing, and brokerage services.[70] Disparate impact discrimination occurs when actions or policies appear to be neutral but adversely affect a protected group of people, without necessarily being intentional.[71] For example, a public housing agency could be in violation of the FHA if it used FRT-enabled surveillance cameras for building access in a manner that resulted in a potential disparate impact, such as for a disproportionate number of residents of a particular race to be mistakenly restricted access to a public housing property.[72] GAO has

[62] GAO, *Rental Housing*, GAO-25-107196, p. 14. See also Rashida Richardson, *Facial Recognition in the Public Sector: The Policy Landscape*, German Marshall Fund of the United States, February 1, 2021, p. 3, http://www.jstor.org/stable/resrep28529.

[63] Information Technology and Innovation Foundation, "Banning Facial Recognition Technology in Public Housing Would Be Misguided, Says Leading Tech Policy Think Tank," press release, July 23, 2019, https://itif.org/publications/2019/07/23/banning-facial-recognition-technology-public-housing-would-be-misguided-says/.

[64] Jennifer A. Kingson, "Elevators of the Future to Employ AI and Facial Recognition," *Axios*, January 4, 2023, https://www.axios.com/2023/01/04/artificial-intelligence-facial-recognition-elevators-otis-schindler-horizontal.

[65] MacMillan, "Eyes on the Poor."

[66] GAO, *Rental Housing*, GAO-25-107196, p. 8.

[67] Gillet Gardner Rosenblith, "Using Surveillance to Punish and Evict Public Housing Tenants Is Not New," *Washington Post*, May 24, 2023, https://www.washingtonpost.com/made-by-history/2023/05/24/public-housing-surveillance/ (hereinafter Rosenblith, "Using Surveillance to Punish and Evict Public Housing Tenants Is Not New").

[68] GAO, *Rental Housing*, GAO-25-107196, p. 14.

[69] NASEM, *Facial Recognition Technology*, p. 77.

[70] For more information on the Fair Housing Act (FHA; 42 U.S.C. §§3601-3631), see CRS Report R48113, *The Fair Housing Act (FHA): A Legal Overview*, by David H. Carpenter.

[71] For more information on disparate impact, see CRS In Focus IF13057, *What Is Disparate-Impact Discrimination?*, by April J. Anderson

[72] Testimony of Chief Responsible AI Officer, National Fair Housing Alliance, Michael Akinwumi in U.S. Commission on Civil Rights, *Civil Rights Implications of the Federal Use of Facial Recognition Technology*, March 8, (continued...)

recommended that the Department of Housing and Urban Development provide detailed written guidance on FRT use in federally assisted housing programs (e.g., permitted uses, renter consent, accuracy, and data management).[73] In addition, some Members have introduced bills, such as H.R. 3060, the No Biometric Barriers to Housing Act of 2025, to prohibit surveillance "or any other use that has an adverse effect on the ability of a tenant to fairly access affordable housing" by limiting the use of FRT in certain federally assisted housing.[74]

Law Enforcement[75]

FRT has been used for a variety of law enforcement purposes, such as to identify victims and generate leads for investigations. This section of the report focuses primarily on recent developments and events pertaining to CBP and Immigration and Customs Enforcement (ICE) because of technical advances in FRT applications and FRT use in immigration and border security in advancing the biometric U.S. entry/exit program.[76]

On October 27, 2025, DHS published a final rule in the *Federal Register* related to the biometric U.S. entry-exit program.[77] This final rule—effective December 26, 2025—made several changes to the implementation of the program, expanding CBP's use of FRT on all noncitizens entering and exiting the U.S. for international travel through airports, seaports, and land crossings.[78] FRT use for U.S. entry and exit is voluntary for U.S. citizens.[79] Travelers are photographed when leaving the United States, and one-to-one FRT verification is used to confirm a match to their identification documents and/or through their partnership with airlines. CBP also uses one-to-many identification FRT to compare "the live photograph of the traveler with a gallery of prepopulated images of participating travelers expected that day at that particular airport."[80] With regard to immigration enforcement, ICE has reportedly been using a one-to-many identification FRT-enabled app, called Mobile Fortify, that uses a smartphone to collect an individual's facial image (or fingerprints). The facial image is sent to CBP's TVS for comparison, demonstrating interagency collaboration for FRT use.[81]

2024, p. 11, https://nationalfairhousing.org/wp-content/uploads/2024/03/Michael-Akinwumi_Testimony_FRT_and_CivilRights_03.08.2024.pdf.

[73] GAO, *Rental Housing*, GAO-25-107196, p. 20.

[74] A version of this bill has been introduced in the 116th, 117th, and 118th Congresses.

[75] For more information on FRT in law enforcement, see CRS Report R46586, *Federal Law Enforcement Use of Facial Recognition Technology*, coordinated by Kristin Finklea. For more information on FRT in immigration, see CRS Report R47541, *Immigration: The U.S. Entry-Exit System*, by Abigail F. Kolker.

[76] CBP, "DHS Announces Final Rule to Advance the Biometric Entry/Exit Program," press release, November 20, 2025, https://www.cbp.gov/newsroom/national-media-release/dhs-announces-final-rule-advance-biometric-entry/exit-program (hereinafter CBP press release).

[77] DHS, "Collection of Biometric Data from Aliens Upon Entry to and Departure from the United States," 90 *Federal Register* 48604, October 27, 2025, https://www.federalregister.gov/documents/2025/10/27/2025-19655/collection-of-biometric-data-from-aliens-upon-entry-to-and-departure-from-the-united-states.

[78] Claire Fahy, "'Biometric Exit' Quietly Expands Across U.S. Airports, Unnerving Some," *New York Times*, September 26, 2025, https://www.nytimes.com/2025/09/26/travel/airports-biometric-exit-program.html. See also CBP press release.

[79] CBP press release.

[80] Privacy and Civil Liberties Oversight Board, *Use of Facial Recognition Technology by the Transportation Security Administration: Staff Report*, May 9, 2025, p. 1, https://documents.pclob.gov/prod/Documents/OversightReport/90964138-44eb-483d-990e-057ce4c31db7/Use%20of%20FRT%20by%20TSA,%20PCLOB%20Report%20(5-12-25),%20Completed%20508,%20May%2019,%202025.pdf.

[81] The DHS Privacy Threshold Analysis (PTA) form for Mobile Fortify is available at https://www.documentcloud.org/ (continued...)

The public and lawmakers have expressed concern about issues related to privacy, consent, misuse, and data security arising from the use of FRT by both CBP and ICE, similar to the issues previously discussed regarding TSA's use of FRT for airport security purposes.[82] During the 119th Congress, some Members have introduced legislation to regulate the use of FRT by law enforcement, including establishing parameters for how, when, and where the technology should be employed.

Travelers are included in biometric data collection efforts or use unless they explicitly request to opt out with CBP. ICE is not required to provide individuals with the opportunity to opt in or opt out of biometric data/photograph collection or use.[83] ICE attempts to conduct FRT scans on citizens and noncitizens. The results of such scans may, in part, lead to detainment from misidentification[84] or noncompliance with being scanned. For example, a lawsuit in Minnesota claims that a U.S. citizen was detained by ICE after agents repeatedly attempted to scan his face.[85] According to DHS, ICE stores and retains each photograph for 15 years.[86] In comparison, CBP may retain pictures in their database for up to 12 hours for U.S. citizens and for up to 75 years for noncitizens who must be enrolled in the DHS Biometric Identity Management System.[87] The length of data storage may amplify some questions relating to privacy, consent, and data security. Members of Congress have raised concerns regarding misuse, including ICE's potential use of FRT as surveillance on citizens and noncitizens.[88]

documents/26209262-mobile-fortify-pta/?ref=404media.co&q=consent&mode=document#document/p4. The Mobile Fortify app is also listed in DHS, "Artificial Intelligence Use Case Inventory," February 11, 2026, https://www.dhs.gov/publication/ai-use-case-inventory-library.

[82] U.S. Congress, House Committee on Homeland Security, "Ranking Member Thompson Introduces Legislation to Curb Unchecked DHS Mobile Biometric Surveillance and Protect Privacy of American Citizens," press release, January 15, 2026, https://democrats-homeland.house.gov/news/legislation/ranking-member-thompson-introduces-legislation-to-curb-unchecked-dhs-mobile-biometric-surveillance-and-protect-privacy-of-american-citizens; and Rep. Pramila Jayapal, "Markey, Jayapal, Merkley, Wyden Introduce Bill to Ban ICE and CBP Use of Facial Recognition Technology Amid Trump's Rapidly Growing Surveillance State," February 5, 2026, https://jayapal.house.gov/2026/02/05/markey-jayapal-merkley-wyden-introduce-bill-to-ban-ice-and-cbp-use-of-facial-recognition-technology-amid-trumps-rapidly-growing-surveillance-state/. See also Kevin Collier et al., "How ICE Agents Are Using Facial Recognition Technology to Bring Surveillance to the Streets," *NBC News*, February 6, 2026, https://www.nbcnews.com/tech/security/ice-agent-facial-recognition-video-protest-movile-fortify-photo-rcna257331.

[83] The DHS PTA form for Mobile Fortify is available at https://www.documentcloud.org/documents/26209262-mobile-fortify-pta/?ref=404media.co&q=consent&mode=document#document/p4. The Mobile Fortify app is also listed in DHS, "Artificial Intelligence Use Case Inventory," February 11, 2026, https://www.dhs.gov/publication/ai-use-case-inventory-library.

[84] Letter from Sen. Edward J. Markey et al. to Todd Lyons, Acting Director of U.S. Immigration and Customs Enforcement (ICE), November 3, 2025, https://www.markey.senate.gov/imo/media/doc/follow-up_to_ice_on_frt.pdf.

[85] Class Action Complaint for Declaratory and Injunctive Relief, Hussen v. Noem, No. 26-324 (D. Minn., January 15, 2026), https://assets.aclu.org/live/uploads/2026/01/COMPLAINT-HUSSEN-v.-NOEM-1.pdf.

[86] The DHS PTA form for Mobile Fortify is available at https://www.documentcloud.org/documents/26209262-mobile-fortify-pta/?ref=404media.co&q=consent&mode=document#document/p4.

[87] CBP press release.

[88] Letter from Sen. Edward J. Markey et al. to Todd Lyons, Acting Director of ICE, September 11, 2025, https://www.markey.senate.gov/imo/media/doc/letter_to_ice_on_mobile_facial_recognition_tech1.pdf. Letter from Sen. Edward J. Markey et al. to Todd Lyons, Acting Director of ICE, November 3, 2025, https://www.markey.senate.gov/imo/media/doc/follow-up_to_ice_on_frt.pdf. See also Sheera Frenkel and Aaron Krolik, "How ICE Already Knows Who Minneapolis Protesters Are," *New York Times*, January 30, 2026, https://www.nytimes.com/2026/01/30/technology/tech-ice-facial-recognition-palantir.html.

State and Local Laws Related to FRT

States and localities have taken a range of legislative approaches regarding FRT.[89] Some states (e.g., Vermont) and cities (e.g., Portland, OR, and Boston, MA) have placed strict limitations on FRT use by public and private entities.[90] Other states have imposed certain conditions or restrictions in particular sectors.[91] For example, the State of New York prohibits the purchase and/or use of FRT in public and private K-12 schools.[92] Most state and local legislation that has been introduced focuses on FRT use by law enforcement.[93] Within the last five years, at least 18 states have considered legislation to regulate FRT use by law enforcement.[94] Some states, such as Oregon and New Hampshire, have banned the use of FRT in combination with law enforcement body cameras.[95] Colorado and Washington require a warrant or court order for FRT use in certain capacities, such as operating continuous surveillance, real-time identification, or tracking, in addition to "an accountability report, data management, security protocols, training procedures and testing" for government usage of FRT.[96]

Selected Policy Considerations for Congress

FRT can enhance the speed, efficiency, and convenience of identification and verification tasks because it is "inexpensive, scalable, and contactless."[97] As the use of FRT has expanded—largely driven by technical advances and offerings of FRT systems by the commercial sector—stakeholders have raised issues regarding sociotechnical implications, such as bias, privacy, and accountability. According to a 2024 RAND survey on the use of FRT by the federal government,

[89] Bobby Allyn, "With No Federal Facial Recognition Law, States Rush to Fill Void," *NPR*, August 28, 2025, https://www.npr.org/2025/08/28/nx-s1-5519756/biometrics-facial-recognition-laws-privacy.

[90] PORTLAND, OR., CITY CODE ch. 34.10, https://www.portland.gov/code/34/10. See also Vermont General Assembly Bill H. 195, https://legislature.vermont.gov/bill/status/2022/H.195, a near-total moratorium on face recognition, prohibiting its use in all situations except for investigations related to sexual exploitation of minors.

[91] Maryland: Md. Lab. & Empl. Code Ann. §3-717, https://mgaleg.maryland.gov/mgawebsite/Laws/StatuteText?article=gle&section=3-717&enactments=false. See also Colorado: Colo. Rev. Stat. §§24-18-301 to 24-18-309, https://content.leg.colorado.gov/sites/default/files/images/olls/crs2024-title-24.pdf. See also Texas 89(R) HB 149 - enrolled version, https://legiscan.com/TX/text/HB149/2025.

[92] New York State Technology Law Section 106-B, https://www.nysenate.gov/legislation/laws/STT/106-B. See also New York State Department of Education, "State Education Department Issues Determination on Biometric Identifying Technology in Schools," press release, September 27, 2023, https://www.nysed.gov/news/2023/state-education-department-issues-determination-biometric-identifying-technology-schools.

[93] Alabama: Code of Ala. §15-10-111, https://alison.legislature.state.al.us/code-of-alabama?section=15-10-111. See also Maine: Title 25, §6001, https://legislature.maine.gov/statutes/25/title25sec6001.html. See also Maryland 2024 SB182, https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/HB0338?ys=2024rs, and HB338, https://mgaleg.maryland.gov/mgawebsite/Legislation/Details/SB0182?ys=2024RS, limits law enforcement's use of facial recognition systems to specific uses and outlines measures; Montana Facial Recognition for Government Use Act 2023 MT S.B. 397, https://bills.legmt.gov/#/bill/20231/LC0067?open_tab=bill; and Utah SB 231 Public Surveillance Prohibition Amendments, https://le.utah.gov/~2024/bills/static/SB0231.html.

[94] Nicole Ezeh et al., "Artificial Intelligence in Law Enforcement: The Federal and State Landscape," National Conference of State Legislatures, January 2025, p. 3, https://documents.ncsl.org/wwwncsl/Criminal-Justice/Law-Enforcement-Fed-Landscape-v02.pdf (hereinafter National Conference of State Legislatures, "Artificial Intelligence in Law Enforcement").

[95] Oregon 133.741, https://www.oregonlegislature.gov/bills_laws/ors/ors133.html, and New Hampshire, https://gc.nh.gov/rsa/html/VII/105-D/105-D-mrg.htm.

[96] National Conference of State Legislatures, "Artificial Intelligence in Law Enforcement," p. 3.

[97] NASEM, *Facial Recognition Technology*, p. 23.

respondents rated factors such as accuracy, privacy, and security as more important than convenience or speed.[98]

This section of the report provides selected policy considerations as Congress determines what, if any, action to take on FRT regulation. Congress might choose to continue to oversee the expansion of FRT use practices, in light of potentially inhibiting innovation and security concerns.[99] Congress might defer to the states to continue regulating FRT use in a state-specific manner. If Congress were to take additional action on FRT regulation, selected policy considerations may include establishing a unified FRT definition and scope or addressing FRT-specific issues, such as accuracy, bias, limited transparency and explainability, privacy, biometric data security, and accountability.

Establishing Unified FRT Definition and Scope

Current laws and guidelines use different FRT definitions and terms, ranging from narrow definitions focused on verification and identification to broader interpretations that include emotion detection, age estimation, and other facial characteristic classifications.

Different definitions for FRT may affect which technologies are captured. Differences in how FRT is defined may influence how the technology is governed across sectors and use cases. For example, legislation with a broader definition for FRT that aims to prohibit its use widely may inadvertently restrict narrower identity verification uses, such as personal smartphone access. Similarly, a definition with a narrower scope may not apply to future FRT developments, especially given its rapidly evolving capabilities. Some other considerations that may affect a definition of FRT include real-time versus retrospective application and voluntary versus involuntary data collection.

Congress may consider whether and how a unified federal definition for FRT might support federal efforts to regulate the use of FRT systems. Such a definition could clarify which systems and functions are covered—including distinctions between FRT-related terms such as *facial analysis* and *facial detection*—to help specify policymakers' intent. Additionally, a standardized definition may need to be revisited periodically or structured flexibly to account for evolving and expanding applications.

Accuracy, Bias, and Explainability of FRT Systems

Congress may engage with issues regarding the accuracy, bias, and explainability of FRT systems by considering how information on such systems (e.g., a model's outputs or how it came to its conclusions) is developed and communicated to stakeholders. This may include conducting oversight into how federal agencies assess system reliability in producing accurate outputs, how information on system performance is documented, and how variations in system outputs are evaluated and communicated to stakeholders. Congress may consider legislation that would require all FRT created or procured by federal agencies to undergo standardized testing and evaluations to provide consistent application of standards that are meant to improve "the accuracy, quality, usability, interoperability, and consistency of identity management system."[100]

[98] Benjamin Boudreaux et al., *Public Perceptions of U.S. Government Uses of Artificial Intelligence*, RAND, March 20, 2024, https://www.rand.org/pubs/research_briefs/RBA691-1.html.

[99] Executive Order 14179 of January 23, 2025, "Removing Barriers to American Leadership in Artificial Intelligence," 90 *Federal Register* 8741, January 31, 2025.

[100] Romine, Testimony in H.Hrg. 116-60.

For example, H.R. 4695, the Facial Recognition Act of 2025, would require law enforcement agencies using FRT to undergo annual accuracy and bias testing conducted by NIST.

Congress may consider how federal evaluations or benchmarks for accuracy could inform commercial practices. Some developers have voluntarily submitted their FRT for evaluation through NIST's FRTE and FATE programs. Congress might consider directing federal agencies to require vendors or funding recipients to conduct such evaluations as a condition of funding.

Congress might encourage the development and implementation of a standard of performance for FRT systems, either generally or for federal use. Among other recommendations, in 2024, the U.S. Commission on Civil Rights recommended that Congress direct and empower NIST to report error rates by demographic group, issue a comprehensive operational testing protocol governing deployment, and require biannual testing of deployed FRT systems to confirm low real-world error rates.[101] Similarly, NASEM has recommended that NIST (1) "sustain a vigorous program of [FRT] testing and evaluation to drive continued improvements in accuracy and reduction in demographic biases" and (2) establish concrete and enforceable technical standards that would clarify minimum image quality requirements, set acceptable error rates, and require consistent accuracy across demographic groups, with stricter thresholds for higher-risk uses.[102]

Accountability and Transparency in FRT Use

Congress might address accountability and transparency in the use of FRT through how federal agencies document, disclose, and oversee their FRT usage. According to GAO, a variety of stakeholders[103] have expressed questions regarding whether federal agencies have the technical expertise needed to properly evaluate their AI systems and make necessary adjustments.[104] Congress may consider requiring federal agencies to assess the need to recruit technical experts or further develop the skills of current employees. Congress may also consider requiring federal agencies that use FRT to clarify roles and responsibilities for system performance and outcomes (e.g., responsibilities of any entity involved in any of the various stages of the system's life cycle)[105] to ensure "effective operations, timely corrections, and sustained oversight."[106]

Finally, Congress might also address FRT use by requiring the private sector to provide disclosures or notices when FRT is used. Congress could direct companies to promote transparency by making information related to FRT systems publicly accessible (e.g., how facial data are collected, stored, shared, and protected, as well as how long they should or would be retained) or by providing notice when any biometric data are being collected.[107] Such actions could create challenges for companies, such as administrative burdens and implementation costs, either of which might slow the pace of innovation. Alternatively, Congress may encourage voluntary disclosures or notices for when FRT is used and biometric data are being collected.

---

[101] U.S. Commission on Civil Rights, "The Civil Rights Implications of the Federal Use of Facial Recognition Technology," p. 102.

[102] NASEM, *Facial Recognition Technology*, p. 110.

[103] Stakeholders include "academic researchers with relevant experience, including federal agency officials, and … advocacy groups that represent communities potentially affected by biometric identification, users of biometric identification technologies, and technology developers and vendors." GAO, *Biometric Identification Technologies*, GAO-24-106293, p. 55.

[104] GAO, *Biometric Identification Technologies*, GAO-24-106293, p. 51.

[105] An AI system's life cycle may include its design, development, deployment, assessment, maintenance, and termination.

[106] GAO, *Artificial Intelligence*, GAO-21-519SP, p. 5.

[107] GAO, *Biometric Identification Technologies*, GAO-24-106293, pp. 46-47.

Author Information

Dominique T. Greene-Sanders
Analyst in Science and Technology Policy

Disclaimer