Congressional Research Service
Informing the legislative debate since 1914

IN FOCUS

Updated August 22, 2024

Biometric Technologies and Global Security

Biometric technologies use unique biological or behavioral attributes—such as DNA, fingerprints, cardiac signatures, voice or gait patterns, and facial or ocular measurements—to authenticate an individual's identity. Although biometric technologies have been in use for decades, recent advances in artificial intelligence (AI) and Big Data analytics have expanded their application. As these technologies continue to mature and proliferate, largely driven by advances in the commercial sector, they will likely hold growing implications for congressional oversight, civil liberties, U.S. defense authorizations and appropriations, military and intelligence concepts of operations, and the future of war.

How are biometric technologies being used today?

Biometric technologies are currently used for a number of congressionally authorized or mandated security applications throughout the U.S. government. For example, the Aviation and Transportation Security Act of 2001 (P.L. 107-71) granted the Transportation Security Administration the authority to employ biometrics for passenger screening and airport access control. Similarly, the Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458) required the Department of Homeland Security to operate a biometric entry and exit data system to verify the identity of foreign nationals seeking to enter or exit the United States. These applications are intended to expedite screening processes and reduce human error rates.

Biometric technologies are also used by law enforcement agencies, such as the Secret Service and Federal Bureau of Investigation, to assist in the investigation of crimes and to identify missing persons and persons of interest. In addition, the Department of Defense (DOD) has used biometric technologies "to identify, target, and disrupt enemy combatants and terrorists" in Iraq, Afghanistan, and elsewhere. The Government Accountability Office has assessed that, between 2008 and 2017, DOD used biometric technologies "to capture or kill 1,700 individuals and deny 92,000 individuals access to military bases."

According to a November 2023 DOD Inspector General (IG) report, some DOD components have been operating biometric technologies that "[do] not have data encryption capabilities" and do not require the "certification of destruction or sanitization of biometric data" when biometric devices are disposed. The report notes that "this could jeopardize force protection by providing adversaries with the biometric information and identities of friendly forces and other individuals assisting the United States." DOD is to update DOD Directive 8521.01E, which establishes the department's policy and bureaucratic responsibilities for biometric technologies, by the first quarter of FY2025 in order to address the IG's findings. Congress may monitor implementation of the directive.

How could biometric technologies be used in the future?

DOD is exploring a range of emerging biometric technologies and biometric applications, including AI techniques that could identify individuals in low-light or otherwise obscured conditions and laser techniques that could identify individuals at distances of around 200 meters. Such techniques could be employed in covert and clandestine operations without an individual's knowledge or consent.

In the future, biometric technologies could be integrated into lethal autonomous weapon systems (LAWS), or weapons capable of selecting and engaging targets without the need for manual human control or remote operation. Such weapons could potentially feature a database containing the biometric identifiers of preapproved human targets; the weapons could then use the database to autonomously locate, select, and engage human targets in communications-degraded or -denied environments where traditional systems may not be able to operate.

Some analysts have argued that this technology application could increase precision in targeting, and thus improve adherence to international humanitarian law (e.g., avoid killing civilians), while others have argued that it is inherently unethical and could violate international humanitarian law. The United States does not currently possess and is not known to be developing LAWS; however, there is no prohibition on their development or the incorporation of biometric technologies into autonomous weapon systems. Weapons manufacturers in both China and Russia have stated that they are developing these systems, which could include biometric features.

Biometric technologies could also be integrated into localized or national data collection and surveillance networks. For example, as Center for Security and Emerging Technology analyst Dahlia Peterson has noted, "[Chinese] officials maintain national DNA databases and extensive video surveillance networks"—augmented by AI-enabled voice and facial recognition technology—to monitor and track individuals within China. These systems could continue to be linked and supplemented with private information such as medical, travel, and purchase history.

Although the Chinese government claims that these biometric applications contribute to predictive policing and public safety, some analysts have argued that they provide a means of imposing censorship and social control and could enable human rights violations. Reports indicate that China

has employed biometric surveillance to monitor ethnic minorities in the Xinjiang Uyghur Autonomous Region and facilitate their detention and internment in "re-education" centers. (Some analysts note that China's application of biometric surveillance systems has not been uniform throughout China, and thus the Xinjiang model is not necessarily representative of China's national plans. Regardless, this model could be deployed nationally in other countries.)

Biometric surveillance systems also could hold implications for traditional military and intelligence operations. According to former CIA Deputy Director for Science and Technology Dawn Meyerriecks, around 30 countries have already deployed biometric surveillance systems that are capable of autonomously tracking foreign military personnel and intelligence operatives. Some estimates suggest that China alone has exported components of these systems to over 80 countries, including authoritarian regimes, such as Venezuela, and U.S. allies, such as the United Kingdom.

Fully integrated, large-scale biometric surveillance networks have not yet been realized; however, as component technologies continue to mature and proliferate, such networks could threaten the privacy or jeopardize the safety of targeted individuals or disrupt U.S. clandestine operations or human intelligence gathering. As a result, U.S. military and intelligence agencies may continue to develop alternative tradecraft and concepts of operation.

How could biometric technologies fail?

Biometric technologies have a number of vulnerabilities that underscore the ethical concerns over their employment and could result in the failure of the technology to perform as anticipated. For example, researchers have repeatedly found that AI-trained facial recognition programs fail disproportionately when used for women and people of color due to both the models and the data on which the programs were trained. Data poisoning, in which an adversary or bad actor seeks to surreptitiously mis-train an opponent's AI, could present additional challenges for AI-trained biometric technologies. If unaddressed, these challenges could result in system failure, potentially leading to violations of civil liberties or international humanitarian law.

Biometric technologies are also vulnerable to presentation attacks (or spoofing), in which a targeted individual uses makeup, prosthetics, or other measures to prevent a biometric system from accurately capturing their biometric identifiers or adjudicating their identity (see **Figure 1**). This could enable individuals such as terrorists or foreign intelligence operatives to thwart biometric security systems.

Some U.S. defense agencies are seeking to develop biometric presentation attack detection technologies. For example, the Intelligence Advanced Research Projects Agency program Odin seeks to provide an automated means of both detecting known presentation attacks and identifying unknown vectors of attack.

Figure 1. Facial Recognition Technologies: How Do They Work?

Sources: @tahkion (image); https://arxiv.org/pdf/2006.05074.pdf.

Note: Facial recognition technology authenticates identity by examining the perceived placement of an individual's facial features, such as the eyes, nose, mouth, and jawline (identified in red—correctly on the left; incorrectly on the right). Evasive measures (e.g., makeup pattern) can cause some facial recognition algorithms to misidentify these features, in turn leading to a failure to correctly adjudicate the individual's identity.

Recent legislative activities

Congress has considered the implications of biometric—specifically facial recognition—technologies in a number of recent legislative provisions. For example, Section 5104 of the FY2021 National Defense Authorization Act (NDAA) (P.L. 116-283) tasks the National AI Advisory Committee with advising the President on "whether the use of facial recognition by government authorities ... is taking into account ethical considerations and ... whether such use should be subject to additional oversight, controls, and limitations." In addition, Section 5708 of the FY2020 NDAA (P.L. 116-92) expresses the sense of Congress that the discriminatory use of facial recognition technologies "is contrary to the values of the United States" and that "the United States Government should not engage in the sale or transfer of facial recognition technology to any country that is using such technology for the suppression of human rights." The section also tasks the Director of National Intelligence with submitting to the congressional intelligence committees a report on the intelligence community's use of facial recognition technologies. Other biometric technologies are not addressed.

Potential questions for Congress

- How should the potential national security benefits of biometric technologies be balanced with civil liberties and the requirements of international humanitarian law? What domestic or international limits, if any, should be placed on the use of biometric technologies or biometric data collection?
- Are biometric technologies being sufficiently tested to ensure their accuracy and to ward against presentation attacks and other countermeasures?
- To what extent are potential U.S. adversaries developing biometric technologies? Are U.S. military and intelligence agencies sufficiently addressing the implications of biometric technologies for tradecraft and concepts of operations?

Kelley M. Sayler, Analyst in Advanced Technology and Global Security

Disclaimer