Congressional Research Service
Informing the legislative debate since 1914

INSIGHT

U.S. Capitol Attack and Law Enforcement Use of Facial Recognition Technology

February 24, 2021

On January 6, 2021, U.S. Capitol security was violently breached while Congress was in session to vote on the certification of the 2020 presidential election. Many participants in the attack reportedly intended to disrupt this process. Some clashed with law enforcement, leaving five dead and many more injured. Some have been charged with violations including crimes against persons and federal property. Some allegedly carried firearms and other weapons. Law enforcement also uncovered explosive devices near Capitol grounds.

Participants, media, and others documented the attack on the Capitol in photographs and video. Law enforcement, such as the Federal Bureau of Investigation (FBI), is seeking this digital content and other evidence to assist its investigation. Among the tools that law enforcement agencies may employ to identify potential criminal suspects depicted in digital content is facial recognition technology (FRT). While some have reported a possible uptick in law enforcement use of FRT following the Capitol attack, the extent to which FRT has been used to identify suspected rioters is unknown.

Law Enforcement Use of FRT

FRT, which compares images of faces using facial geometry, is one biometric tool employed by law enforcement. FRT can be used to generate suspect leads, identify victims, sort faces in photos that are part of forensic evidence, and verify the identity of inmates being released from prison. FRT is generally used by law enforcement in *one-to-many searches* (comparing features of a *probe* photo with those in a database of images) to produce a gallery of potential suspects ranked by similarity—not a single affirmative match.

FBI Use of FRT

The FBI operates two FRT programs: (1) the Next Generation Identification–Interstate Photo System (NGI-IPS), largely supporting state and local law enforcement; and (2) the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit, supporting FBI investigations.

- NGI-IPS contains criminal mugshots, and the system allows authorized law enforcement users to search probe photos of unknown persons against faces in the database for potential investigative leads.

- The FACE Services Unit searches probe photos against faces in NGI-IPS and other authorized federal and state facial recognition systems.

A facial recognition search alone cannot provide law enforcement with a positive identification; the results must be manually reviewed and compared by an officer trained in facial comparison. The FBI prohibits law enforcement agencies from taking action (e.g., making an arrest) based solely on the results of a search in NGI-IPS.

There is a patchwork of FRT systems used by federal, state, and local law enforcement agencies around the country—including those investigating the Capitol attack. Each has its own database of faces against which probes may be compared, and law enforcement agencies may have differing policies governing FRT use. For instance, federal law enforcement agencies and authorized users of their FRT systems must generally follow established FRT policies and guidelines, which may not apply to state and local law enforcement agencies' FRT systems.

Federal law enforcement agencies have previously used FRT to identify individuals suspected of criminal activity associated with protests. Federal agencies investigating the Capitol attack have not confirmed specific use of FRT but have confirmed reviewing photo and video footage. State and local law enforcement, and individuals and companies, may also use FRT to help identify suspected Capitol rioters—tips that they may provide to law enforcement.

Concerns over the use of FRT include the accuracy or reliability of FRT systems, public notification regarding the use of FRT, and policies governing law enforcement agencies' use of the technology. Concerns surfaced following reports that Clearview AI, a company that developed image-search technology used by law enforcement agencies around the country, had amassed a database of over 3 billion images against which *probe* photos could be compared. Some concerns have manifested in federal, state, and city efforts to prohibit or bound law enforcement agencies' use of FRT. Further, some companies producing facial recognition software have enacted barriers to law enforcement using their technologies.

Legislative Considerations

FRT can be a powerful investigative tool for law enforcement. But some observers have voiced concern about the technology's current and prospective use. While FRT's reliability has improved over time, the accuracy rates of FRT systems vary, particularly in identifying persons in certain demographic groups, leading some to express concern regarding possible misidentification. Some have also expressed concern that FRT—when paired with other tools and databases that contain millions of face images—could enable surveillance that encroaches on personal privacy and civil liberties. Others contend that these concerns are overstated and may not justify curtailing law enforcement's use of this investigative tool.

Several bills in the 116th Congress sought to regulate the use of FRT by the government or commercial entities, with most seeking to constrain its use. Several bills would also have sought to influence how state and local police use FRT by conditioning the receipt of criminal justice grants upon compliance with certain guidelines. Since the Capitol attack, there has been considerable discussion of whether police use of FRT to identify suspected participants will inform policymakers' assessment of whether to encourage or constrain the police use of FRT in the future.

Congress has not enacted legislation specifically addressing FRT. Outside the border security context, the most pertinent federal laws address the collection and storage of personal data by government agencies or commercial entities generally, though many such laws do not constrain information shared for law enforcement purposes. State and local regulation of FRT, in turn, varies considerably. While many state and local governments widely employ FRT, others expressly prohibit or limit its use. And although the Constitution provides baseline parameters for FRT's use by government actors, these considerations may be more relevant to assessments of the technology's use in a particular investigation than to FRT's general development and deployment.

Author Information

Kristin Finklea
Specialist in Domestic Security

Kelsey Y. Santamaria
Legislative Attorney

Disclaimer

This document was prepared by the Congressional Research Service (CRS). CRS serves as nonpartisan shared staff to congressional committees and Members of Congress. It operates solely at the behest of and under the direction of Congress. Information in a CRS Report should not be relied upon for purposes other than public understanding of information that has been provided by CRS to Members of Congress in connection with CRS's institutional role. CRS Reports, as a work of the United States Government, are not subject to copyright protection in the United States. Any CRS Report may be reproduced and distributed in its entirety without permission from CRS. However, as a CRS Report may include copyrighted images or material from a third party, you may need to obtain the permission of the copyright holder if you wish to copy or otherwise use copyrighted material.