Negative: Facial Recognition Technology Warrant Act

By David W. Helton

**Resolved: The United States Federal Government should substantially reform the use of Artificial Intelligence technology**

The Affirmative plan will require federal agencies to, in most circumstances, obtain a warrant before using facial recognition technology (FRT) to track a person. The bill also mandates that the FRT algorithms used by federal agencies be tested by the NIST for bias. There are a few problems with this bill. First, FRT can’t be used as the sole evidence to arrest or convict a suspect. Second, agencies like the FBI already test there FRT systems for bias. Third, the bill has a lot of solvency issues, and requiring warrant s may not lead to any sort of accountability. Finally, using FRT systems provides evidence and leads that aren’t attainable otherwise, and restricting the use of FRT may hamper law enforcement’s ability to effectively use FRT.

Negative: Facial Recognition Technology Warrant Act 2

INHERENCY 2

FRT is already being regulated 2

FBI’s use of FRT is secure 2

FBI has incentive and regulations in place to ensure its FRT systems aren’t biased 3

FBI prohibits law enforcement from an arrest solely based on FRT and AI. Manual reviews are required 3

FRT is used only for leads. Manual review is required. 3

FRT photos can’t be used to prove identity and lots of safeguards exist to prevent erroneous identification 4

MINOR REPAIR 4

Good FRT algorithms exist that are accurate / without bias. Let’s improve oversight to make sure we’re using them 4

HARMS / SIGNIFICANCE 4

FRT is far better at identifying suspects than humans are 4

FBI is removing FRT bias. Big improvements in accuracy have been made in recent years (now over 99%) 5

FRT is improving 5

Bias is being eliminated in FRT 5

SOLVENCY 6

FRT Warrant Act doesn’t block facial recognition for identification purposes 6

Bill doesn’t provide judicial oversight 6

Bill doesn’t prevent misuse of FRT 6

Bill doesn’t protect privacy rights 7

Bill doesn’t require warrants in all circumstances 7

Time restrictions on warrants are meaningless 7

DISADVANTAGES 8

1. Weakens law enforcement 8

A. FRT provides leads 8

B. FRT provides information that isn’t attainable otherwise 8

C. Impact: Crime and public safety. 8

 Negative: Facial Recognition Technology Warrant Act

INHERENCY

FRT is already being regulated

Julie Carr Smyth 2021 (journalist, Associated Press. BA and MA in Journalism from Ohio State Univ) May 5, 2021 “States push back against use of facial recognition by police” <https://abcnews.go.com/Politics/wireStory/states-push-back-facial-recognition-police-77510175> (Accessed 22 July 2021)

At least seven states and nearly two dozen cities have limited government use of the technology amid fears over civil rights violations, racial bias and invasion of privacy. Debate over additional bans, limits and reporting requirements has been underway in about 20 state capitals this legislative session, according to data compiled by the Electronic Privacy Information Center.

FBI’s use of FRT is secure

 Ernest J. Babcock 2015 (Senior Component Official for Privacy at the FBI; former Deputy General Counsel for the Investigative and Administrative Law Branch, Deputy Assistant Director, and Privacy and Civil Liberties Officer.) Date Approved: May 1, 2015 “Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit” <https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit> (accessed 22 Aug 2021) (the period is missing after “FACE Services Unit” in the original; no text has been removed in this card)

The FACE Services Unit uses government-issued biometric thumb drives to transfer information between systems and perform a security scan each time data is transferred. The supervisors conduct random checks of the thumb drives to ensure that content is disposed of in accordance with established security procedures. Biometrics Images Specialists (BIS) are assigned a Biometric Thumb Drive that is stored in a locked cabinet located within the FACE Services Unit. All the Biometric Thumb Drives are blank except for when a BIS is assigned live case work. Upon completion of each assigned case, the BIS are mandated by FACE Services and IT Security Policy to remove/delete any and all information from the Biometric Thumb Drive and place the Biometric Thumb Drive back in the locked cabinet daily. No data is retained after the completion of the live case work. All BIS and BIS Supervisors are required to sign an internal FACE Services acknowledgement letter that outlines the rules for handing Biometric Thumb Drives used for processing work in the FACE Services Unit
Every member of the FACE Services Unit has undergone privacy, security, classification, and investigatory training to ensure that information is properly handled. Frequent and random compliancy checks are performed by the BIS Supervisors to ensure that all policies are followed.

FBI has incentive and regulations in place to ensure its FRT systems aren’t biased

 Ernest J. Babcock 2015 (Senior Component Official for Privacy at the FBI; former Deputy General Counsel for the Investigative and Administrative Law Branch, Deputy Assistant Director, and Privacy and Civil Liberties Officer.) Date Approved: May 1, 2015 “Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit” <https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit> (accessed 22 Aug 2021)

A person under arrest or the subject of a criminal or national security investigation generally has no opportunity or right to refuse the collection of biometrics, including photographs. The privacy risks associated with lack of notice to affected individuals about the collection, maintenance, and use of probe photos are mitigated somewhat by the general notice to the public via the FBI’s published SORNs, PIAs, and other Privacy Act notices. The risk of erroneous information is mitigated because the FBI has a substantial interest in ensuring the accuracy of information in the system, and in taking action to correct any erroneous information of which it may become aware. Additionally, the risk is mitigated because the maintenance and dissemination of information must comply with the provisions of any applicable law, regulation, or policy, including the Privacy Act. Title 28 C.F.R. part 16, subpart A, provides general guidance on access to information in FBI files pursuant to the Freedom of Information Act, and 28 C.F.R. part 16, subpart D, provides general guidance regarding access to, and amendment of, information in FBI files pursuant to the Privacy Act.

FBI prohibits law enforcement from an arrest solely based on FRT and AI. Manual reviews are required

Congressional Research Service 2021 (Kristin Finklea - Specialist in Domestic Security at CRS. Analyst in domestic security at the domestic social policy. Kelsey Y. Santamaria - Legislative Attorney at the CRS. Former Judicial Law Clerk for the US District Court of the Western District of Texas. JD and BA in International Relations from Univ of California.) 24 Feb 2021 “U.S. Capitol Attack and Law Enforcement Use of Facial Recognition Technology” <https://crsreports.congress.gov/product/pdf/IN/IN11614> (accessed 24 July 2021)

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.

FRT is used only for leads. Manual review is required.

Ryan Lucas 2019 (journalist for NPR; former foreign correspondent for The Associated Press based in Poland, Egypt and Lebanon. Bachelor's degree from William and Mary, master's degree from Jagiellonian University in Krakow, Poland.) 21 August 2019 “How A Tip — And Facial Recognition Technology — Helped The FBI Catch A Killer” <https://www.npr.org/2019/08/21/752484720/how-a-tip-and-facial-recognition-technology-helped-the-fbi-catch-a-killer> (accessed 31 Aug 2021)

Facial recognition "remains an investigative lead only," FBI Deputy Assistant Director Kimberly Del Greco testified to Congress in 2017. "The candidates must be further reviewed by specialized face examiners and/or the relevant investigators."

 FRT photos can’t be used to prove identity and lots of safeguards exist to prevent erroneous identification

 Ernest J. Babcock 2015 (Senior Component Official for Privacy at the FBI. He has served as Deputy General Counsel for the Investigative and Administrative Law Branch, Deputy Assistant Director, and Privacy and Civil Liberties Officer.) Date Approved: May 1, 2015 “Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit” <https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit> (accessed 22 August 2021)

Finally, the return of candidate photos to the FBI agent or analyst may result in the potential misidentification of a subject. However, this risk is greatly mitigated by both the automated and manual face recognition comparison of the probe photo against the candidate photos. In many instances, no candidate photos are returned because none meet a high enough quality threshold. When a candidate photo is returned to an investigator, he or she is clearly informed that the photo serves only as an investigative lead and may not be used to prove identity. The FACE Services Unit biometric images specialists receive significant training on face recognition and on the handling of evidence. They only consider the candidate photo in conjunction with all other evidence, such as biographic information, physical evidence, and victim and witness statements.

MINOR REPAIR

Good FRT algorithms exist that are accurate / without bias. Let’s improve oversight to make sure we’re using them

Congressional Research Service 2020 (Kristin Finklea - Coordinator Specialist in Domestic Security.  Laurie A. Harris - Analyst in Science and Technology Policy. Abigail F. Kolker -  Analyst in Immigration Policy. John F. Sargent Jr. -  Specialist in Science and Technology Policy.) October 27, 2020 “Federal Law Enforcement Use of Facial Recognition Technology” <https://fas.org/sgp/crs/misc/R46586.pdf> (Accessed 24 July 2021)

A December 2019 NIST study of both one-to-many identification search algorithms and one-toone verification algorithms found that FRT algorithms’ accuracy rates can vary by demographic factors such as age, sex, and race. For example, false positive rates tended to be higher for Asian and African American faces compared to those of Caucasians, which may be due to the data used to train the algorithm; an explanation that the NIST study did not explore. However, NIST noted that there is wide variation among algorithms, with some producing significantly fewer errors, and errors of different types, than others. Policymakers may wish to exercise oversight over the specific FRT algorithms employed by federal law enforcement agencies, and the data on which those systems are trained, as they evaluate the accuracy and use of facial recognition. They may also debate whether or how to provide legislative direction aimed at maximizing the accuracy of FRT algorithms used by federal law enforcement entities. In attempting to maximize accuracy, developers and users of FRT must weigh the consequences of errors (false positives and false negatives) for different communities and decide which error measure is of higher priority to minimize, depending on how the threshold is set.

HARMS / SIGNIFICANCE

FRT is far better at identifying suspects than humans are

Jan Lunter 2020 (the co-founder and CEO of Innovatrics, which has been developing and providing fingerprint recognition solutions since 2004. He is also author of a fingerprint analysis and recognition algorithm that regularly ranks among the top in comparison tests (NIST PFT II, NIST Minex); graduated from the Télécom ParisTech Univ. in France.) October 20, 2020 “Beating the bias in facial recognition technology” <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7575263/> (Accessed 22 July 2021)

A 2001 analysis of police cases found that cross-racial identifications carried out by humans were correct a mere 46% of the time – far below even the least-accurate facial recognition algorithms. In short, it's important to note that while reducing bias in FRT remains a key priority, the technology already significantly outperforms witness-based methods of identification.

FBI is removing FRT bias. Big improvements in accuracy have been made in recent years (now over 99%)

Sujit Raman 2020 (Nearly a dozen years as a federal prosecutor, former Associate Deputy Attorney General at the U.S. Department of Justice. Advisor to the Attorney General and Deputy Attorney General on cyber-related criminal and national security investigations and prosecutions) 15 Sept 2020 "Five Principles That Inform the Justice Department’s  Use of Facial Recognition Technology" <https://www.justice.gov/opa/speech/associate-deputy-attorney-general-sujit-raman-delivers-remarks-community-oriented> (accessed 22 Aug 2021)

We have a moral obligation to study demographic differentials in connection with Facial Recognition Technology.  We must approach this issue honestly, and with due regard for evidence-based reviews.  We in the federal government will continue to ensure that demographic differentials and inaccuracies are constantly being tested, quantified, and mitigated using an evidence-based approach.  In fact, it is precisely that approach that led to the progress reflected in the 2018 NIST Face Recognition Vendor Test, in which top algorithms experienced a failure (i.e., a false positive or a false negative match) on NIST-provided data inputs only 0.2% of the time, compared with a 4% failure rate in 2014 — an improvement by a factor of 20 in only four years. Through its partnership with NIST, the FBI in 2019 upgraded its NGI IPS algorithm; the selected vendor’s facial recognition algorithm performs at an accuracy rate that exceeds 99%. Going forward, the FBI plans, in collaboration with NIST, to test its NGI IPS facial recognition technology annually.  Much work remains to be done.  But the remarkable progress we have seen in the accuracy of FRT in just a few years is cause for optimism.

FRT is improving

Congressional Research Service 2020 (Kristin Finklea - Coordinator Specialist in Domestic Security.  Laurie A. Harris - Analyst in Science & Technology Policy. Abigail F. Kolker -  Analyst in Immigration Policy. John F. Sargent Jr. -  Specialist in Science & Technology Policy.) 27 Oct 2020 “Federal Law Enforcement Use of Facial Recognition Technology” <https://fas.org/sgp/crs/misc/R46586.pdf> (accessed 24 July 2021) (brackets added)

With respect to its 2018 FRVT [Face Recognition Vendor Test], NIST reported that: The 2018 FRVT tested 127 facial recognition algorithms from the research laboratories of 39 commercial developers and one university, using 26 million mugshot images of 12 million individuals provided by the FBI. The 2018 FRVT measured the accuracy and speed of one-to-many facial recognition identification algorithms. The evaluation also contrasted mugshot accuracy with that from lower quality images. The findings, reported in NIST Interagency Report 8238, showed that massive gains in accuracy have been achieved since the FRVT in 2013, which far exceed improvements made in the prior period (2010-2013).

Bias is being eliminated in FRT

Clare Garvie and Jonathan Frankle 2016 (Garvie - a law fellow at the Center on Privacy & Technology at Georgetown Law. B.A., Barnard College, Columbia University; J.D., Georgetown. She is also an Adjunct Professor of Law. Frankle - staff technologist at the Center on Privacy & Technology at Georgetown Law. He is a fifth-year PhD student at MIT.) April 7, 2016 “Facial-Recognition Software Might Have a Racial Bias Problem” <https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/>  (Accessed 28 July 2021)

The National Institute of Standards and Technologies (NIST) conducts voluntary tests of [facial-recognition vendors](http://www.nist.gov/itl/iad/ig/frvt-home.cfm) every four years. In 2010, NIST [observed](http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905968) that accuracy rates had improved tenfold between each round of testing, a dramatic testament to the technology’s rapid advances.

SOLVENCY

FRT Warrant Act doesn’t block facial recognition for identification purposes

Alfred Ng 2019 (A privacy and surveillance reporter for the Markup. He previously worked as a senior reporter for CNET, covering cybersecurity and privacy, and a reporter for the New York Daily News) November 14, 2019 “Facial recognition surveillance would require warrant under bipartisan bill” <https://www.cnet.com/news/facial-recognition-surveillance-would-require-warrant-under-bipartisan-bill/> (Accessed 17 August 2021)

The Facial Recognition Technology Warrant Act was introduced by Sen. Chris Coons, a Democrat from Delaware, and Sen. Mike Lee, a Republican from Utah. The bill calls for federal agencies like the FBI and US Immigration and Customs Enforcement to obtain a warrant if they want to use facial recognition for ongoing surveillance, like tracking a person's whereabouts for longer than 72 hours.

**[END QUOTE. HE GOES ON LATER IN THE ARTICLE TO WRITE QUOTE:]**

The bill introduced Thursday wouldn't stop the use of facial recognition for identification purposes, which is how ICE and the FBI have been tapping the tech in several cases. The proposed legislation would specifically require a warrant to use facial recognition to follow a person around.

Bill doesn’t provide judicial oversight

Alfred Ng 2019 (A privacy and surveillance reporter for the Markup. He previously worked as a senior reporter for CNET, covering cybersecurity and privacy, and a reporter for the New York Daily News) November 14, 2019 “Facial recognition surveillance would require warrant under bipartisan bill” <https://www.cnet.com/news/facial-recognition-surveillance-would-require-warrant-under-bipartisan-bill/> (Accessed 17 August 2021)

"It has gaping loopholes that authorize the use of facial recognition for all kinds of abusive purposes without proper judicial oversight," said Evan Greer, Fight for the Future's deputy director. "It's good to see that Congress wants to address this issue, but this bill falls utterly short."

Bill doesn’t prevent misuse of FRT

Fight for the Future 2019 (nonprofit advocacy group in the area of digital rights related to copyright legislation, as well as online privacy and censorship on the Internet.) November 14, 2019 “We scanned thousands of faces in DC today to show why facial recognition surveillance should be banned” <https://fightfortheftr.medium.com/we-scanned-thousands-of-faces-in-dc-today-to-show-why-facial-recognition-surveillance-should-be-3360958a76f1> (Accessed 30 August 2021)

While our action was still going on, news reports started to emerge that Senators Coons and Lee had introduced a new bill related to facial recognition. Unfortunately, this bill falls far short of the type of legislation we need. It would do nothing to prevent the type of invasive facial recognition surveillance that we conducted today. And it contains gaping loopholes that authorize government and law enforcement to deploy facial recognition surveillance in all kinds of abusive ways.

Bill doesn’t protect privacy rights

Andrew Wyrich citing Neema Singh Guliani 2019 (the deputy tech editor at the Daily Dot. Andrew has written for USA Today, NorthJersey.com, and other newspapers and websites. His work has been recognized by the Society of the Silurians, Investigative Reporters & Editors, and the Society of Professional Journalists (SPJ). Neema Singh Guliani - senior legislative counsel at American Civil Liberties Union) 14 Nov 2019 “Why today’s new facially recognition bill is being called ‘woefully’ inadequate”  <https://www.dailydot.com/debug/facial-recognition-technology-warrant-act/> (Accessed 30 August 2021)

This bill would authorize the invasive, persistent, and dystopian surveillance that communities across the country have rejected,” Guliani said. “The bill falls woefully short of protecting people’s privacy rights and is inconsistent with existing Supreme Court precedent. Congress should put brakes on this technology, not ineffective band-aids.”

Bill doesn’t require warrants in all circumstances

Andrew Wyrich 2019 (the deputy tech editor at the Daily Dot. Andrew has written for USA Today, NorthJersey.com, and other newspapers and websites. His work has been recognized by the Society of the Silurians, Investigative Reporters & Editors (IRE), and the Society of Professional Journalists (SPJ).) November 14, 2019 “Why today’s new facially recognition bill is being called ‘woefully’ inadequate” <https://www.dailydot.com/debug/facial-recognition-technology-warrant-act/> (Accessed 30 August 2021)

The Facial Recognition Technology Warrant Act was introduced by Sen. Chris Coons (D-Del.) and Sen. Mike Lee (R-Utah). The technology’s use—especially among law enforcement—has been under fierce criticism from both advocacy groups and even some lawmakers in recent months.

**[END QUOTE. HE GOES ON LATER IN THE ARTICLE TO WRITE QUOTE:]**The bill, however, would allow law enforcement to use the technology without a warrant during “exigent circumstances,” according to the summary.

Time restrictions on warrants are meaningless

Andrew Wyrich 2019 (the deputy tech editor at the Daily Dot. Andrew has written for USA Today, NorthJersey.com, and other newspapers and websites. His work has been recognized by the Society of the Silurians, Investigative Reporters & Editors (IRE), and the Society of Professional Journalists (SPJ).) November 14, 2019 “Why today’s new facially recognition bill is being called ‘woefully’ inadequate” <https://www.dailydot.com/debug/facial-recognition-technology-warrant-act/> (Accessed 30 August 2021)

The bill tries to “balance” the “security benefits and privacy concerns that come with this new technology,” according to a summary of the bill released by the senators. It would require federal law enforcement agencies to obtain a warrant when using facial recognition for “ongoing public surveillance of an individual” for anything more than 72 hours. It would also limit the warrants to 30 days.

**[END QUOTE. HE GOES ON LATER IN THE ARTICLE TO WRITE QUOTE:]**That group, Fight for the Future, criticized the bill amid its ongoing protest. “It’s almost impossible to think of a scenario where this bill would do anything,” the group tweeted. “It requires a warrant if you want to use facial recognition to track a specific person for more than 72 hours. If cops are doing that there are many other ways they can monitor someone.”

DISADVANTAGES

1. Weakens law enforcement

A. FRT provides leads

 Ernest J. Babcock 2015 (Senior Component Official for Privacy at the FBI. He has served as Deputy General Counsel for the Investigative and Administrative Law Branch, Deputy Assistant Director, and Privacy and Civil Liberties Officer.) Date Approved: May 1, 2015 “Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit” <https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit> (Accessed 22 August 2021) (brackets in original)

By using face recognition technology to search probe photos for matching candidate photos, the FACE Services Unit provides unique and specialized value to the FBI’s mission to fight crime [REDACTED].  In many instances, face recognition results in information that is not available with any other investigative method. To date, more than 6,000 face recognition leads have been returned to FBI agents and other investigators. Most investigations are ongoing, but two arrests have been made as a result of leads provided by the FACE Services Unit, and two victims from a violent crimes case have been located.

B. FRT provides information that isn’t attainable otherwise

 Ernest J. Babcock 2015 (Senior Component Official for Privacy at the FBI. He has served as Deputy General Counsel for the Investigative and Administrative Law Branch, Deputy Assistant Director, and Privacy and Civil Liberties Officer.) Date Approved: May 1, 2015 “Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit” <https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments/facial-analysis-comparison-and-evaluation-face-services-unit> (Accessed 22 August 2021)

As listed below, the FBI has statutory authority to collect, preserve, and exchange biographic and biometric information for criminal and national security purposes. In line with that authority, the FACE Services Unit provides investigative lead support to FBI personnel by comparing facial images of subjects who are the focus of active FBI investigations and assessments. By using face recognition technology to search probe photos for matching candidate photos, the FACE Services Unit provides unique and specialized value to the FBI’s mission to fight crime and terrorism. In many instances, face recognition results in information that is not available with any other investigative method. Candidate photos are used by FBI agents for a variety of reasons, including further investigation of a potential subject, to determine/verify the identity of a subject already in custody, to discover an alias that the subject may be using, to identify associates of the subject, and to eliminate potential subjects.

C. Impact: Crime and public safety.

Congressional Research Service 2020 (Kristin Finklea - Coordinator Specialist in Domestic Security.  Laurie A. Harris - Analyst in Science and Technology Policy. Abigail F. Kolker -  Analyst in Immigration Policy. John F. Sargent Jr. -  Specialist in Science and Technology Policy.) October 27, 2020 “Federal Law Enforcement Use of Facial Recognition Technology” <https://fas.org/sgp/crs/misc/R46586.pdf> (Accessed 24 July 2021)

FRT can be a powerful tool for law enforcement in protecting public safety—potentially assisting law enforcement in identifying a criminal suspect, crime victim, or other person of interest. The adoption of FRT can also increase the efficiency of certain government processes. FRT is deployed, for instance, at international borders to verify individuals’ claimed identities, reducing the need to manually check paper travel documents.