Connolly, Miller U.S.
5-22-19

ITIF | **INFORMATION TECHNOLOGY & INNOVATION FOUNDATION**

Chairman Elijah Cummings
Committee on House Oversight and Reform
2157 Rayburn House Office Building
Washington, DC 20515

Ranking Member Jim Jordan
Committee on House Oversight and Reform
2157 Rayburn House Office Building
Washington, DC 20515

May 21, 2019

Dear Chairman Cummings and Ranking Member Jordan,

On behalf of the Information Technology and Innovation Foundation (ITIF)—a non-profit, non-partisan think tank—I would like to thank you and the other members of the House Committee on Oversight and Reform for organizing a hearing on the topic of facial recognition and its impact on civil rights and liberties. ITIF appreciates the opportunity to submit the following statement for your consideration.

Facial recognition is a rapidly evolving technology that offers numerous potential benefits, both for the public and private sectors. Facial recognition uses a computer to automatically match similar faces, either by searching for similar images in a database (one-to-many) or by confirming whether two images match (one-to-one). While there is more Congress can do to ensure government use of facial recognition is fair and reliable, recent calls for bans or moratoriums on law enforcement use of facial recognition are misguided and will only undercut efforts to make police agencies more efficient and effective in protecting local communities.

HOW FACIAL RECOGNITION TECHNOLOGY HELPS KEEP COMMUNITIES SAFE

There are many potential ways police can use facial recognition technology. As an investigative tool, facial recognition can help police identify witnesses, suspects, and other persons of interest in a crime. Without facial recognition, police must do these searches manually, such as combing through mug shot photos or asking the public to help identify someone, a process that is slow, inaccurate, and expensive.[1] Indeed, facial recognition will make it much more feasible to investigate low-dollar crimes, such as car break-ins and

[1] Chris Adzima, "Using Amazon Rekognition to Identify Persons of Interest for Law Enforcement," AWS Machine Learning Blog, June 15, 2017, https://aws.amazon.com/blogs/machine-learning/using-amazon-rekognition-to-identify-persons-of-interest-for-law-enforcement/.

package thefts from doorsteps, which often go unaddressed. Although, digital searches are only part of the investigative process, and police still must have probable cause to make arrests.

Police are also using facial recognition to help stop crimes. For example, some police departments, such as in Fort Worth, Texas, are using facial recognition technology to search for missing children online who may have become possible victims of sex trafficking.[2] Facial recognition can also help police improve security at schools, stadiums, and other public places. For example, if police receive a credible threat of a person planning a shooting or bombing at one of these venues, they can use real-time facial recognition to quickly monitor the crowd and receive an alert if the person of interest arrives.

Finally, police can use facial recognition to improve the security of their own systems and facilities, such as to control access to their buildings or to provide an added layer of security when authenticating users to their computer systems.

In the future, there may also be opportunities to use facial recognition to help respond in real-time to amber alerts for missing children and silver alerts for people with dementia. Or police may use facial recognition in the field, to let officers know who is approaching them—an application that could be used to improve community relations.

PUBLIC SUPPORTS FACIAL RECOGNITION TECHNOLOGY FOR PUBLIC SAFETY

Although San Francisco, California has recently made headlines by passing a ban on the use of facial recognition technology for law enforcement, the public generally opposes such radical measures. In a poll last December, the Center for Data Innovation found that only one in four Americans (26 percent) think government should strictly limit the use of facial recognition technology—and that support drops even further if it would come at the expense of public safety.[3] Fewer than one in five Americans (18 percent) would agree with strictly limiting the technology if it came at the expense of public safety, while a solid majority (55 percent) would disagree.

---

[2] Lisa Lacy, "This Startup Is Using Facial Recognition To Fight Human Trafficking," AdWeek, May 31, 2018, https://www.adweek.com/digital/this-startup-is-using-facial-recognition-to-fight-human-trafficking/.

[3] Daniel Castro and Michael McLaughlin, "Survey: Few Americans Want Government to Limit Use of Facial Recognition Technology, Particularly for Public Safety or Airport Screening," (Center for Data Innovation, January 7, 2019), https://www.datainnovation.org/2019/01/survey-few-americans-want-government-to-limit-use-of-facial-recognition-technology-particularly-for-public-safety-or-airport-screening/.

Older Americans were more likely to oppose government limits on the technology. For example, 52 percent of 18- to 34-year-olds opposed limitations that come at the expense of public safety, compared to 61 percent of respondents ages 55 and older. In addition, women were more likely to oppose limits than men. For example, only 14 percent of women support strictly limiting facial recognition if it comes at the expense of public safety, versus 23 percent of men.

The survey also asked respondents whether government should limit surveillance cameras, since they are integral to many applications of facial recognition technology. Overall, Americans were more likely to support limiting surveillance cameras (36 percent) than facial recognition technology (26 percent). If it would come at the expense of public safety, then just 18 percent of Americans would agree with limiting surveillance cameras and the same percentage would agree for facial recognition. These findings suggest that what little support there is for limiting facial recognition technology is related to existing support for limiting the use of surveillance cameras.

FACTS ABOUT RACE AND GENDER BIAS IN FACIAL RECOGNITION HAVE BEEN MISCONSTRUED

While the public generally supports facial recognition technology, there have been mounting critiques about potential racial or gender bias in the use of the technology. These critiques should be taken seriously, but also carefully scrutinized because the headlines often do not accurately represent the facts.

First, there are many different facial recognition systems on the market, and the accuracy and error rates of these systems vary. Some systems perform better than others, including in their accuracy rates across race, gender, and age. For example, the most recent results of the one-to-one facial recognition matching test from the National Institute of Standards and Technology (NIST) shows the top-performing algorithm having a lower error rate on black females than on white males.[4]

Second, many of the claims about racial bias are misconstruing the facts. For example, some of the critiques, especially those citing the MIT Media Labs, conflate "facial analysis" (where a system attempts to discern certain characteristics about a face, such as the subject's age or gender) with facial recognition.[5]

---

[4] Patrick Grother, Mei Ngan, and Kayee Hanaoka, "Ongoing Face Recognition Vendor Test (FRVT), Part 1: Verification" (National Institute of Standards and Technology, April 12, 2019), https://www.nist.gov/sites/default/files/documents/2019/04/15/frvt_report_2019_04_12.pdf.

[5] Daniel Castro, "Note to Press: Facial Analysis is Not Facial Recognition," Innovation Files, January 27, 2019, https://itif.org/publications/2019/01/27/note-press-facial-analysis-not-facial-recognition.

Third, many of the critiques about racial bias in facial recognition algorithms refer to older technologies. Newer versions of these facial recognition systems perform more accurately, and the technology continues to improve over time.[6] For example, one of the recent critiques of Amazon Rekognition referred to an older version of the system.

Fourth, the accuracy of facial recognition systems depends on a range of variables, including the quality of the images used and the confidence thresholds for determining matches. Some of the critiques have focused on facial recognition systems that use low thresholds, thereby artificially inflating error rates. For example, an oft-cited ACLU study compared photos of members of Congress to a mug shot database and found a number of false positives. However, the ACLU used a lower confidence threshold than recommended.[7] The ACLU used a confidence threshold of 80 percent, which is suitable for some uses, such as tagging friends on social media, but Amazon recommends using a 99 percent threshold when higher levels of accuracy are necessary, such as in law enforcement. Indeed, Dr. Matt Wood, who oversees machine learning at Amazon Web Services, says that the ACLU's reported error rate would drop from 5 percent to zero at this higher confidence level.[8]

Finally, these critiques overlook the fact that humans are often more biased in recognizing faces than computers are, particularly when they are looking for people of different races than themselves.[9] Facial recognition technology can mitigate some of these human biases, including among law enforcement.

STEPS TO IMPROVE OVERSIGHT AND ACCOUNTABILITY

There are a number of steps Congress can take to improve oversight and accountability of facial recognition use by law enforcement.

First, Congress should expand its evaluation of commercial facial recognition systems. Importantly, NIST should include testing of cloud-based facial recognition systems. Currently, all algorithms must be submitted

---

[6] Daniel Castro, "Note to Press: Facial Analysis is Not Facial Recognition," Innovation Files, January 27, 2019, https://itif.org/publications/2019/01/27/note-press-facial-analysis-not-facial-recognition.

[7] Daniel Castro and Michael McLaughlin, "Banning Police Use of Facial Recognition Would Undercut Public Safety," (Information Technology and Innovation Foundation, July 30, 2018), https://itif.org/publications/2018/07/30/banning-police-use-facial-recognition-would-undercut-public-safety.

[8] Matt Wood, "Thoughts on Machine Learning Accuracy," AWS Machine Learning Blog, July 27, 2018, https://aws.amazon.com/blogs/machine-learning/thoughts-on-machine-learning-accuracy/.

[9] See, for example, Daniel Wright, Catherine Boyd, and Colin Tredoux, "Inter-facial contact and the own-race bias for face recognition in South Africa and England," Applied Cognitive Psychology, March 14, 2003, https://onlinelibrary.wiley.com/doi/abs/10.1002/acp.898.

as pre-compiled software libraries, which means many cloud providers cannot participate in these evaluations. Expanding to include these providers would be useful as many state and local law enforcement agencies are using cloud-based services. Independent public testing of these facial recognition systems will encourage more competition in the market and accelerate improvements in existing systems, since law enforcement agencies will likely be able to switch easily between various cloud-based vendors.

Second, Congress should direct NIST to expand its set of training and evaluation data for facial images and include race, gender, and age as key diversity metrics. By funding the creation of additional and more diverse training and evaluation datasets for facial recognition, Congress can spur developers to further reduce any differences in accuracy across different demographics and reduce concerns about bias.

Third, Congress should direct DOJ to work with NIST to set performance standards for facial recognition technology, including for accuracy and error rates for race and gender. Congress should require that any federal grants to state and local law enforcement that are used to procure facial recognition technology meet or exceed these performance standards. This will ensure police departments do not waste tax dollars on ineffective systems or ones with significant racial bias.

Fourth, Congress should direct the departments of Justice and Homeland Security to develop best practices on government use of facial recognition technology, including operational guidance and oversight protocols. In addition, the National Institute of Justice should create best practices for state and local law enforcement to improve their use of facial recognition technology. This guidance should include recommendations for how to publicly disclose when law enforcement uses the technology, the types of data sources used for images, and retention policies.

Finally, Congress should continue to consider broader oversight on appropriate police behavior and legislation to uphold civil liberties. For example, it should clarify the appropriateness of police surveillance of political protests, regardless of the type of technology used for surveillance. And it should continue to provide oversight of racial bias in law enforcement and the criminal justice systems, especially racial disparities in police use of force among communities of color. Policymakers should also evaluate whether there is a need to affirmatively establish a warrant requirement to track the movements of individuals by any means, including with facial recognition systems, mobile phones, or license plate readers. By addressing these broader issues, Congress can address many of the underlying concerns that are not tied to the use of this particular technology.

CONCLUSION

It is always important for Congress to consider the impact of new technologies and ensure there are proper guardrails in place to protect society's best interests. In the case of facial recognition technology, there are many clear opportunities to use the technology to improve public safety. Attempts to limit police use of the technology are misguided. A better approach is to establish guidance and policies that would limit potential misuse and abuse of facial recognition technology but allow police to use the latest technologies to keep citizens and communities safe.

Sincerely,

Daniel Castro
Vice President, Information Technology and Innovation Foundation
Director, ITIF's Center for Data Innovation