

An Open Letter to Congress on Facial Recognition*

September 26, 2019

Dear Member of Congress:

Facial recognition technology is one of many technologies that law enforcement can use to help keep communities safe. Facial recognition systems have improved rapidly over the past few years, and the best systems perform significantly better than humans.¹ Today facial recognition technology is being used to help identify individuals involved in crimes, find missing children, and combat sex trafficking. As the technology continues to improve, there will be even more opportunities in the future to use the technology as an investigative tool to solve crimes; as a security countermeasure against threats in airports, schools, and other public venues; and as a means to securely identify individuals at ports of entry. Indeed, travelers are already responding positively to biometric entry/exit programs that allow them to pass swiftly and securely through airports.²

While polls consistently show that Americans trust law enforcement to use facial recognition technology responsibly, some groups have called for lawmakers to enact bans on facial recognition technology.³ While we agree that it is important to have effective oversight and accountability of these tools to uphold and protect civil liberties, we disagree that a ban is the best option to move forward. Bans would keep this important tool out of the hands of law enforcement officers, making it harder for them to do their jobs efficiently, stay safe, and protect our communities.

We are writing to encourage you to consider many of the viable alternatives to bans so that law enforcement can use facial recognition technology safely, accurately, and effectively. These alternatives may include expanding testing and performance standards, the development of best practices and guidance for law enforcement, and additional training for different uses of the technology.

¹ P. J. Phillips et al., "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms," Proceedings of the National Academy of Sciences, June 12, 2018, <https://www.pnas.org/content/pnas/115/24/6171.full.pdf>.

² "Air Passengers Believe Technology Can Improve Travel," Xenophon Analytics, July 1, 2019, <https://xenophonstrategies.com/technology-can-improve-travel/>; "Delta expands optional facial recognition boarding to new airports, more customers," Delta, June 19, 2019, <https://news.delta.com/delta-expands-optional-facial-recognition-boarding-new-airports-more-customers>; "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/>.

³ "More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly," Pew Research Center, September 5, 2019, <https://www.pewinternet.org/2019/09/05/more-than-half-of-u-s-adults-trust-law-enforcement-to-use-facial-recognition-responsibly/>.

There are many individuals from law enforcement, industry, academia, and civil society who stand ready to work with lawmakers to craft appropriate safeguards for this technology. We encourage you to continue to work with these experts to find solutions and compromises that will allow law enforcement agencies to adopt and test this important technology with appropriate oversight.

Thank you for your consideration.

Sincerely,

Organizations

Acuant, Inc.
Arm Inc.
AWARE
Cognitec
Computing Technology Industry Association (CompTIA)
Consumer Technology Association
Electronic Security Association
HID Global
iBeta QA
ID Technology Partners, Inc.
IJIS Institute
Innovatrics s.r.o.
Information Technology and Innovation Foundation
International Biometrics + Identity Association
Iris ID Systems Inc
JENETRIC
National Police Foundation
National Troopers Coalition
NEC Corporation of America
NetChoice
Rank One Computing Corporation
Security Industry Association (SIA)
TechNet
Thales USA
Vision-Box

Individuals

Affiliations are listed for identification purposes only
Maria Cardiello, IJIS Institute
Daniel Castro, Center for Data Innovation
Warren Champ, Ledios Inc
Paulo Da Silva, Cognitec Systems Pty Ltd
Dongpyo Hong, Global PD

Roger Kelesoglu, IBIA member
Joshua Kolchins, Vision Box Systems, Inc
Tovah LaDier, IBIA
James Lewis, Center for Strategic and International Studies
Doug Maccaferri, Cognitec Systems Corporation
John Mears, IBIA
Leonard Pratt, Qualcomm Technologies Inc
Ivan Quinn, Secure Planet
Diane Ragans, IJIS Institute
Cristian Tamas, TypingDNA

**This letter has been jointly prepared by the International Biometrics + Identity Association (IBIA) and the Information Technology and Innovation Foundation (ITIF).*