



Artificial intelligence software tools tested for demographic impact

[eSignature and ePayment News and Trends](#)

20 December 2019

By: Margo H. K. Tank | David Whitaker | Andrew Grant | Liz Caires

On December 19, the National Institute of Standards and Technology (NIST), a federal agency within the Department of Commerce, released a study titled “Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects.” The study describes and quantifies demographic differentials for contemporary face recognition algorithms. Essentially, the purpose of the study was to measure how accurately face recognition software tools identify people of varied sex, age and racial background.

NIST conducted tests to quantify demographic differences for nearly 200 face recognition algorithms from nearly 100 developers, using four collections of photographs with more than 18 million images of more than 8 million people. The report found “empirical evidence for the existence of a wide range of accuracy across demographic differences in the majority of the current face recognition algorithms that were evaluated” and detailed errors that are possible in face verification and identification and their impacts, include racial and gender bias.

The results of the report are intended to inform policymakers and to help software developers better understand the performance of their algorithms. Earlier this year, the Artificial Intelligence Task Force of the House Financial Services Committee held a [hearing](#), “Perspectives on Artificial Intelligence: Where We Are and the Next Frontier in Financial Services.” In the hearing, members of Congress and witnesses acknowledged AI’s potential to increase

access to financial services and discussed concerns that AI could result in discrimination against minorities and other underserved groups.

At the state level, to date, seven states [(1) Arizona, Ariz. Rev. Stat. § 18-551; (2) Arkansas, Arkansas Code § 4-110-103; (3) California, Cal. Civ. Code § 1798.140; (4) Illinois, 740 ILCS 14/1, *et seq*; (5) Michigan, Mich. Comp. Laws §§ 445.63; (6) Texas, Tex. Bus. & Com. Code Ann. § 503.001; and (7) Washington, Wash. Rev. Code §§ 19.375.010, *et seq*.] have laws that regulate the use and collection of biometric data in some capacity, which in some state laws include biometric information such as a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.

While there have been no outright prohibitions on use, it is clear that both state and federal lawmakers will be considering these issues in the next decade, including with respect to AI use in connection with among other things, credit decisions and data security and privacy.

You may also enjoy the latest issue of our publication AI Outlook previewing a coming congressional hearing on facial recognition technology.

AUTHORS



Margo H. K. Tank

Partner
Washington, DC | T: +1 202 799 4000
margo.tank@dlapiper.com



David Whitaker

Partner
Chicago | T: +1 312 368 4000
david.whitaker@dlapiper.com



Andrew Grant

Associate
Washington, DC | T: +1 202 799 4000
andrew.grant@dlapiper.com



Liz Caires

Attorney
Dallas | T: +1 214 743 4500
liz.caires@dlapiper.com
