

Research finds US adults have context-specific views on biometric technology use

November 23 2021, by Samantha Chavanic



Credit: Pixabay/CC0 Public Domain

As the application of facial recognition and DNA technologies increases across industries and domains, questions arise concerning the public's comfort with biometric modalities, the acceptability of using biometrics

in various societal contexts, and the public's trust in public and private entities using biometric technologies. An international team of researchers set out to understand perspectives about biometric technologies held by a representative sample of adults across the United States.

Over two weeks in late 2020, the research team surveyed 4,048 adults, a sampling that reflected the U.S. population with respect to geographic region, age, gender, racial and ethnic background, educational attainment, household income and political leanings. The team asked participants to rank six types of biometrics—fingerprint, voice sample, facial image, eye scan, hand geometry and DNA—indicating what they were comfortable with organizations using for any purpose.

The team published the results in *IEEE Transactions on Technology and Society*. Of the [survey respondents](#), nearly 41% ranked fingerprints as the biometric they were most comfortable with for wide use. As the team expected, [survey results](#) showed a correlation between prior experience with [biometric technologies](#) and increased comfortability, although it is not possible to infer whether comfort influenced those prior experiences or vice versa. When asked to rank the biometric technologies based on level of comfort, most survey participants indicated they are very or somewhat comfortable with all the technologies—74.8% for fingerprint use, 66.2% for voice samples, 63% for hand geometry use, 61.1% for facial imaging and 60.6% for eye scans. The lowest percentage of a very or somewhat comfortable rating was reported for DNA at 55.6%. Demographics showed little to no effect on reported comfort levels.

Those who said they were not very comfortable or completely uncomfortable with wide use of biometrics stated reasons including invasion of privacy, wanting to know how the information will be used, what policies exist around information storage, and fear of governmental oversight.

"It was somewhat surprising that perspectives did not appear to be influenced strongly by demographics such as gender or racial and ethnic background, despite growing awareness of the biases of facial recognition technologies and their applications," said senior author Jennifer K. Wagner, assistant professor of law, policy and engineering at Penn State. "We are wondering how diversity of perspectives might be masked due to varying informational needs (on biometric technologies) that we did not consider in this study."

In addition to these general questions, half the survey participants were asked to rank specific biometrics used to perform specific tasks, such as fingerprint or facial recognition to unlock smartphones, on a comfortability scale. The majority, 67.1%, indicated comfort with the increasingly common biometric task. Of the seven scenarios presented to the participants, the majority indicated being uncomfortable with biometric technology used by [retail stores](#) to track store movement and later apply in targeted advertising, in reconnection scenarios completed by people search companies, homeowner associations applying technology to track sidewalk and street movements and customer loyalty program applications.

"Policy is often running to keep up with tech and science developments," said first author Sara Huston Katsanis, head of the Genetics and Justice Laboratory at Ann & Robert H. Lurie Children's Hospital of Chicago and research assistant professor of pediatrics at Northwestern University Feinberg School of Medicine. "Often technology developments proceed when they are feasible, without pause for what the ramifications are of that [technology](#). Just because we *can* do something doesn't mean we *should*. Biometric technologies have vast potential to simultaneously benefit and harm individuals and groups. It is our goal to understand what those benefits and risks are in various applications so that the public can make informed context-specific decisions on what is deemed acceptable uses of emerging biometrics."

The team found that the specific type of biometric, whether facial imaging or DNA, did not seem to influence the perceived trust in public and private entities' use of biometrics, but context did matter. Slim majorities of respondents trusted [law enforcement agencies](#), intelligence agencies, researchers and scientists and [health care workers](#) with the collection and use of two types of biometric data, but slight majorities of respondents distrusted advertisers, tech companies, retailers and governments.

The researchers plan to investigate how contextual factors help shape perspectives, according to Wagner.

"Given how widely biometric technologies in general and facial analytics in particular are being used in society, it is surprising that so little is known about the perspectives held by adults in the United States about them," Wagner said. "We need to try to make sure that the biometric technologies, practices and the policies surrounding [biometric](#) data take more nuanced considerations into account."

More information: Sara H. Katsanis et al, U.S. Adult Perspectives on Facial Images, DNA, and Other Biometrics, *IEEE Transactions on Technology and Society* (2021). [DOI: 10.1109/TTS.2021.3120317](https://doi.org/10.1109/TTS.2021.3120317)

Provided by Pennsylvania State University

Citation: Research finds US adults have context-specific views on biometric technology use (2021, November 23) retrieved 23 April 2024 from <https://techxplore.com/news/2021-11-adults-context-specific-views-biometric-technology.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.