Biometric ID technologies 'inherently fallible', new report says

24 September 2010

Biometric systems -- designed to automatically recognize individuals based on biological and behavioral traits such as fingerprints, palm prints, or voice or face recognition -- are "inherently fallible," says a new report by the National Research Council, and no single trait has been identified that is stable and distinctive across all groups. To strengthen the science and improve system effectiveness, additional research is needed at virtually all levels of design and operation.

"For nearly 50 years, the promise of biometrics has outpaced the application of the technology," said Joseph N. Pato, chair of the committee that wrote the report and distinguished technologist at Hewlett-Packard's HP Laboratories, Palo Alto, Calif. "While some biometric systems can be effective for specific tasks, they are not nearly as infallible as their depiction in popular culture might suggest. Bolstering the science is essential to gain a complete understanding of the strengths and limitations of these systems."

Biometric systems are increasingly used to regulate access to facilities, information, and other rights or benefits, but questions persist about their effectiveness as security or surveillance mechanisms. The systems provide "probabilistic results," meaning that confidence in results must be tempered by an understanding of the inherent uncertainty in any given system, the report says. It notes that when the likelihood of an imposter is rare, even systems with very accurate sensors and matching capabilities can have a high false-alarm rate. This could become costly or even dangerous in systems designed to provide heightened security; for example, operators could become lax about dealing with potential threats.

The report identifies numerous sources of uncertainty in the systems that need to be considered in system design and operation. For example, biometric characteristics may vary over an individual's lifetime due to age, stress, disease, or other factors. Technical issues regarding calibration of sensors, degradation of data, and security breaches also contribute to variability in these systems.

Biometric systems need to be designed and evaluated relative to their specific intended purposes and the contexts in which they are being used, the report says. Systems-level considerations are critical to the successful deployment of biometric technologies. Effectiveness depends as much on factors such as the competence of human operators as it does on the underlying technology, engineering, and testing regimes. Well-articulated processes for managing and correcting problems should be in place.

The report notes that careful consideration is needed when using biometric recognition as a component of an overall security system. The merits and risks of biometric recognition relative to other identification and authentication technologies should be considered. Any biometric system selected for security purposes should undergo thorough threat assessments to determine its vulnerabilities to deliberate attacks. Trustworthiness of the biometric recognition process cannot rely on secrecy of data, since an individual's biometric traits can be publicly known or accessed. In addition, secondary screening procedures that are used in the event of a system failure should be just as well-designed as primary systems, the report says.

The report identifies several features that a biometric system should contain. Systems should be designed to anticipate and plan for errors, even if they are expected to be infrequent. Additional research is needed in all aspects of design and operation, from studying the distribution of biometric traits in given populations to understanding how people interact with the technologies. In addition, social, legal, and cultural

factors can affect whether these systems are effective and accepted, the report says.

Provided by National Academy of Sciences

APA citation: Biometric ID technologies 'inherently fallible', new report says (2010, September 24) retrieved 20 June 2021 from https://phys.org/news/2010-09-biometric-id-technologies-inherently-fallible.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.