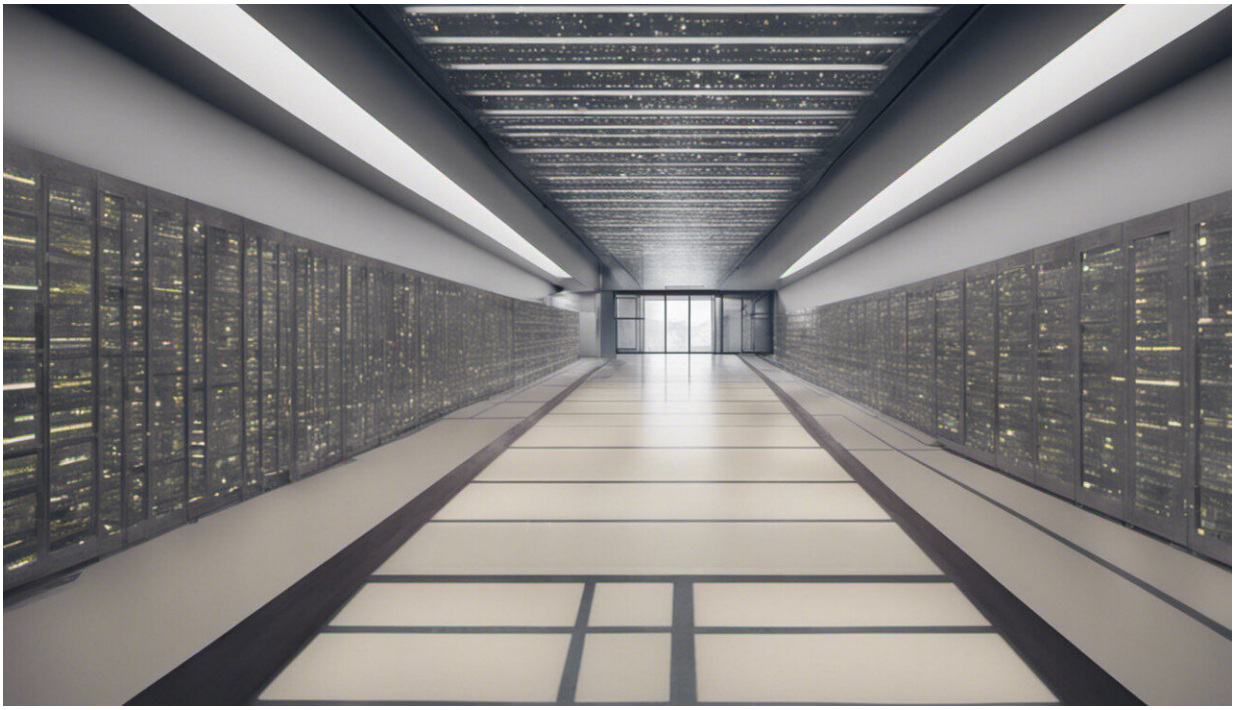
The trouble with taking biometric technology into schools

January 7 2016, by Brian Patton, University Of Oxford



Credit: AI-generated image (disclaimer)

More usually criticised for their conservative approach to technology, schools are becoming proving grounds for some of the latest biometrics and portable biomedical engineering devices. Or so it would appear, with St Mary's School Ascot, an independent girls school in Berkshire, joining an estimated 3,500 schools to have introduced biometric security

systems, in this case a biometric finger-vein scanner which promises to uniquely identify pupils. But in embracing technology such as biometrics, schools may be gambling with their pupils' identity.

The tennis ball-sized device verifies pupils' identity and confirms their attendance at lunch or in lessons. The scanner works by shining infrared light through the top of the finger onto a scanner plate below. As haemoglobin in the blood scatters more light than the surrounding tissue, the sensor plate will detect a shadow image of the blood vessels in the finger. This image forms the credential that is used to identify an individual, reduced by a computer to a set of key parameters that should be unique for each user. And here we see the potential problems with biometric technologies, regardless of the implementations.

A good way of securely identifying someone is to rely on more than one piece of identifying information. For example, for credit or debit card purchases a shop will require the card (something you have) and your PIN (something you know). This is known as multi-factor authentication and makes it harder to steal identities or the valuables associated with them.

Biometric scanners all try to address the first factor, something you have. They also trade on convenience as – barring accidents – we effortlessly carry around the body part they measure. But even without getting into gruesome measures, it is not an impossible task for thieves to acquire what they need.

Credit: Iakobchuk Vacheslav/EPA

Fingerprints, for example, have proven to be easy to acquire, with German politicians having theirs swiped. For other biometric data it's important to remember that what is being matched within the computer is not, say, one fingerprint against another. It is a set of data drawn from the features of the scanned body part – a numerical abstraction. Steal this key and you have effectively stolen that part of the person.

This is where the "multi" part of the multi-factor authentication comes in. If you need both my fingerprint and a password that I know, then my identity is still safe. But that part of my personal biometrics – fingerprint, retina or iris scan, facial recognition data – is nevertheless

compromised and untrustworthy. I may have ten fingerprints, but without a central register or someone to act as a trust broker, the thieves can still set up false identities with third parties. My bank may know not to trust my left-index fingerprint for identification, but does the bank next door?

No doubt with the best of intentions, schools are taking these security and technological risks and exposing pupils' personal biometric data. By introducing this fingerprint scanning system St Mary's appears to be using only the biometrics data: they are trusting, opaque, black-box technological systems over the sense of their own trained human staff. If it's a requirement that staff are also present when the scanners are used, then what is the system's benefit? While the school claims that the biometric data will be destroyed when pupils leave the school, a data breach will mean these type of scans will be untrustworthy for the pupils – for the rest of their lives.

And therein lies another issue: with the potential for life-long consequences, are pupils, some below the age of 16, competent to opt in to such a scheme? And what of those who opt out? It's one thing to ask adults to weigh up the balance between convenience and risk, but there are two likely issues that would make this harder in schools. There is an inbalance of power between those wanting to implement the technology and those subject to it. This raises serious concerns about informed consent – perhaps one of the reasons why in 2012 using biometrics was banned in English state schools without parents' consent.

Likewise, the emotions that arise in discussions of child safety make it difficult to challenge anything that claims to improve it. The change in attitude of schools toward technology so that they equip their pupils with the skills needed for the 21st century is laudable. But it should not compromise their pupils in the long term for the sake of questionable, and at best short-term benefits for staff and administrators.

This article was originally published on The Conversation. Read the original article.

Source: The Conversation

Citation: The trouble with taking biometric technology into schools (2016, January 7) retrieved 23 May 2024 from https://phys.org/news/2016-01-biometric-technology-schools.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.