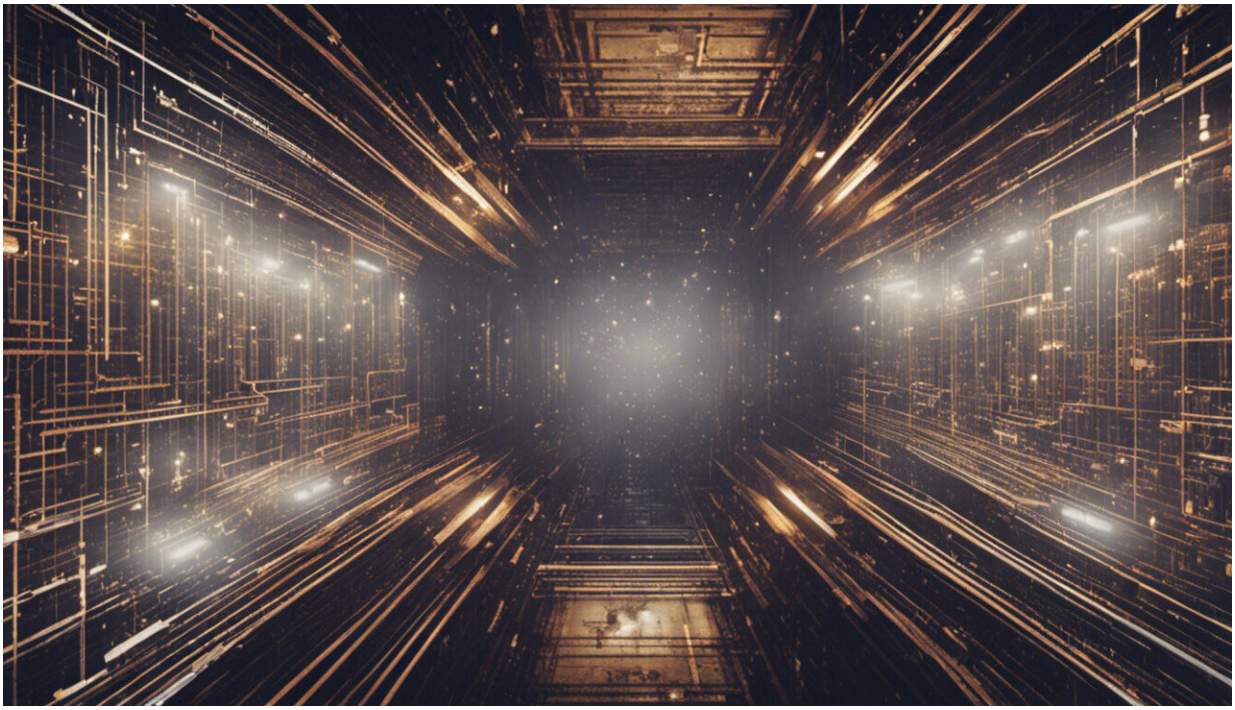
Iris scanners can now identify us from 40 feet away

May 22 2015, by Anne-Marie Oostveen And Diana Dimitrova



Credit: AI-generated image (disclaimer)

Biometric technologies are on the rise. By electronically recording data about individual's physical attributes such as fingerprints or iris patterns, security and law enforcement services can quickly identify people with a high degree of accuracy.

The latest development in this field is the scanning of irises from a distance of up to 40 feet (12 metres) away. Researchers from Carnegie Mellon University in the US demonstrated they were able to use their iris recognition technology to identify drivers from an image of their eye captured from their vehicle's side mirror.

The developers of this technology envisage that, as well as improving security, it will be more convenient for the individuals being identified. By using measurements of physiological characteristics, people no longer need security tokens or cumbersome passwords to identify themselves.

However, introducing such technology will come with serious challenges. There are both legal issues and public anxiety around having such sensitive data captured, stored, and accessed.

Social resistance

We have researched this area by presenting people with potential future scenarios that involved biometrics. We found that, despite the convenience of long-range identification (no queuing in front of scanners), there is a considerable reluctance to accept this technology.

On a basic level, people prefer a physical interaction when their biometrics are being read. "I feel negatively about a remote iris scan because I want there to be some kind of interaction between me and this system that's going to be monitoring me," said one participant in our research.

But another serious concern was that of "function creep", whereby people slowly become accustomed to security and surveillance technologies because they are introduced gradually. This means the public may eventually be faced with much greater use of these systems than they would initially agree to.

For example, implementing biometric identification in smart phones and other everyday objects such as computers or cars could make people see the technology as useful and easy to operate, This may increase their willingness to adopt such systems. "I could imagine this becoming normalised to a point where you don't really worry about it," said one research participant.

Such familiarity could lead to the introduction of more invasive long-distance recognition systems. This could ultimately produce far more widespread commercial and governmental usage of biometric identification than the average citizen might be comfortable with. As one participant put it: "[A remote scan] could be done every time we walk into a big shopping centre, they could just identify people all over the place and you're not aware of it."

Legal barriers

The implementation of biometric systems is not just dependent on user acceptance or resistance. Before iris-scanning technology could be introduced in the EU, major data protection and privacy considerations would have to be made.

The EU has a robust legal framework on privacy and data protection. These are recognised as fundamental rights and so related laws are among the highest ranking. Biometric data, such as iris scans, are often treated as special due to the sensitivity of the information they can contain. Our respondents also acknowledged this: "I think it's a little too invasive and to me it sounds a bit creepy. Who knows what they can find out by scanning my irises?"

Credit: AI-generated image (disclaimer)

Before iris technology could be deployed, certain legal steps would need to be taken. Under EU law and the European Convention on Human Rights, authorities would need to demonstrate it was a necessary and proportionate solution to a legitimate, specific problem. They would also need to prove iris recognition was the least intrusive way to achieve that goal. And a proportionality test would have to take into account the risks the technology brings along with the benefits.

The very fact that long-range iris scanners can capture data without the collaboration of their subject also creates legal issues. EU law requires individuals to be informed when such information was being collected, by whom, for what purposes, and the existence of their rights surrounding the data.

Another issue is how the data is kept secure, particularly in the case of iris-scanning by objects such as smart phones. Scans stored on the device and/or on the cloud for purposes of future authentication would legally require robust security protection. Data stored on the cloud tends to move around between different servers and countries, which makes preventing unauthorised access more difficult.

The other issue with iris scanning is that, while the technology could be precise, it is not infallible. At its current level, the technology can still be fooled (see video above). And processing data accurately is another principle of EU data protection law.

Even if we do find ourselves subject to unwanted iris-scanning from 40 feet, safeguards for individuals should always be in place to ensure that they do not bear the burden of technological imperfections.

Provided by The Conversation