Businesses are harvesting our biometric data. The public needs assurances on security

July 10 2024, by Kamran Mahroof, Amizan Omar and Irfan Mehmood

Credit: Pixabay/CC0 Public Domain

Imagine walking through a bustling railway station. You're in a hurry, weaving through the crowd, unaware that cameras are not just watching you but also recognizing you.

These days, our biometric data is valuable to businesses for security purposes, to enhance customer experience or to improve their own efficiency.

Biometrics, are unique physical or behavioral traits, and are part of our everyday lives. Among these, facial recognition is the most common.

Facial recognition technology stems from a branch of AI called computer vision and is akin to giving sight to computers. The technology scans images or videos from devices including CCTV cameras and picks out faces.

The system typically identifies and maps 68 specific points known as facial landmarks. These create a digital fingerprint of your face, enabling the system to recognize you in real time.

Face landmarks include the corners of the eyes, the tip of the nose and the edges of the lips. They help to create a mathematical representation of the face without storing the entire image, enhancing both privacy and efficiency.

From supermarkets to car parks and railway stations, CCTV cameras are everywhere, silently doing their job. But what exactly is their job now?

Businesses may justify collecting biometric data, but with power comes responsibility and the use of facial recognition raises significant transparency, ethical and privacy concerns.

When even police use of facial recognition can be deemed unethical, then the business justification becomes less convincing, especially as little is known how businesses store, manage and use data.

Capturing and storing biometric data without consent could violate our

rights, including protection against surveillance and retention of personal images.

Balancing safety, efficiency and privacy rights is a complex ethical choice for a businesses.

As consumers, we may often be reluctant to share our personal information. Yet facial recognition poses more serious risks, such as deepfakes and other impersonation threats.

Take for instance the recent revelation that Network Rail has been secretly monitoring thousands of passengers using Amazon's AI software. This surveillance highlights a critical issue: the need for transparency and stringent regulations, even when a company is watching us with the aim of improving services. A Network Rail spokesperson said, "When we deploy technology, we work with the police and security services to ensure that we're taking proportionate action, and we always comply with the relevant legislation regarding the use of surveillance technologies."

One of the core challenges is the issue of consent. How can the public ever give informed consent if they are constantly monitored by cameras and unaware of who is storing and using their biometric data?

This fundamental problem underscores the difficulty in resolving privacy concerns. Businesses face the daunting task of obtaining clear, informed consent from people who might not even know they are being observed.

Without transparent practices and explicit consent mechanisms, it's nearly impossible to ensure that the public is truly aware of and agrees to the use of their biometric data.

Think about your digital security. If your password gets stolen, you can change it. If your credit card is compromised, you can cancel it. But your face? That's permanent. Biometric data is incredibly sensitive because it cannot be altered once it's compromised. This makes it a high-stakes game when it comes to security.

If a database is breached, hackers could misuse this data for identity theft, fraud, or even harassment.

Another issue is algorithmic bias and discrimination. If data is used for decision-making, how can companies ensure that diverse and sufficient data is included to train the algorithm?

Companies might use biometric data for authentication, personalized marketing, employee monitoring and access control. There is a significant risk of gender and racial biases if the algorithm is primarily trained on data from a homogenous group, such as white males.

Companies should also be ensuring that digital bias is not perpetuated. Failing to do so may lead to societal inequalities.

Legislation and awareness

As facial recognition becomes more common, the need for robust legislation becomes urgent. Laws must mandate clear consent before capturing anyone's biometric data. They should also set strict standards for how this data is stored and secured to prevent breaches.

It's equally crucial that the public becomes more aware of the issue. While people are becoming more conscious about data protection, facial recognition often flies under the radar. It's invisible in our everyday lives, and many don't realize the risks and ethical issues. Educating the public is vital.

Incorporating the principles of responsible AI into the deployment of facial recognition technology would be a good place to start. Responsible AI emphasizes fairness, accountability, transparency and ethics. This means that AI systems, including facial recognition, should be designed and used in ways that respect human rights, privacy and dignity.

However, businesses might not necessarily prioritize these principles if they are not being held accountable by regulatory bodies or the public.

Transparency is a cornerstone of responsible AI. If organizations using facial recognition remain secretive about their practices, we cannot trust them with our biometric data.

Companies armed with only your personal information can be very powerful in terms of manipulative marketing. It takes only "one like" for bespoke campaigns to target you very accurately.

But now, political parties such as the PTI in Pakistan have embraced vision-AI technology to allow leader Imran Khan to campaign despite serving a prison sentence.

Visual data capturing and analysis are particularly critical compared to non-visual data because they provide richer, more intimate and more immediate insights into human behavior and identity.

That's why its growing use by businesses raises so many concerns about privacy and consent. While the public remains unaware of the extent to which their visual data is being captured and utilized, their information will be vulnerable to misuse or exploitation.

Provided by The Conversation