What if your emotions were tracked to spy on you?

Recent reports of celebrity singer, Taylor Swift, deploying facial recognition technology to spot stalkers at her concerts raised many eyebrows. What started out as a tool to unlock your smartphone or tag photos for you on social media is surreptitiously becoming a means of monitoring people in their daily lives without their consent. What impact and implications are facial recognition technology applications likely to have, and what can be done to ensure the fair engagement of this technology with its users and the public at large?

These days you can take out cash, check in at airports and pay bills just using your face. This is possible thanks to facial recognition (FR) technology, the latest ground-breaking development in data-driven technology. FR technology compares the detected face in a digital image or a video frame with large databases in order to identify or authenticate a person. Not only can this biometric technology be used to identify you, it can also determine your age, gender and sexual orientation. Even more significantly, perhaps, it might soon be used to detect what you are thinking and track your every move, without your consent.

© Elnur / Shutterstock.com

FR technology is linked to emotion recognition, also referred to as affect recognition, which it is claimed can be used to identify moods, emotions and personality, etc. This information could then be used, for instance, to monitor mental health, detect fraudulent insurance claims, influence people's shopping experiences through personalised advertising, or to spot potential shoplifters. Through emotion recognition, technology based on images or videos of faces also offers the potential to monitor students' classroom participation, or help employers recruit workers. It is therefore not surprising that demand for FR-enabled applications and the value they offer is booming, leading to a rapid expansion of related industries.

Possible impacts and developments

FR technology is one of the main building blocks of smart environments, and could underpin the smart cities of the future. With FR technology embedded, a smart environment can identify a user, interpret his or her actions or facial expressions and then interact through personalised messages based on the moods and emotions interpreted. The power of FR lies in its potential to be built into various smart environments with a view to providing personalised services.

Facial recognition applications are being piloted by law enforcement authorities at airports and borders to help them address terrorist threats, cross-border crime, irregular migration and child trafficking. Applications are also being pilot tested for use in targeted and mass surveillance and tracking in streets, at football matches and music festivals, at carnivals and at transport hubs. Police have already used this technology to spot people on mental health watch lists, identify protesters at arms fairs and detect stalkers.

FR-enabled applications already facilitate faster entry at events for people who have opted in, as well as payment at restaurants, or for insurance or other purchases. FR is opening up new opportunities for advertisers, retailers and marketers to personalise marketing. Data about customers' movements and behaviour, combined with mood analysis using emotion recognition, may soon be used by retailers to present customers with customised advertisements. Emotion recognition may also one day be used by recruiters when hiring, or by employers to monitor the moods of employees and adapt the working environment empathetically, or even to track employees' work engagement patterns.

Author: Lieve Van Woensel with Nissy Nevil, Scientific Foresight Unit (STOA)

In healthcare, emotion recognition technology could eventually be used in the diagnosis and treatment of autism, in suicide prevention and in the early detection of Parkinson's disease. In medical emergencies, mobile applications enabled by FR technology could be used to identify a patient who is unconscious and unable to communicate relevant medical conditions, and to identify features such as age or gender, check if the patient's medical history already exists in the database, and retrieve the associated medical information. FR might also be used in the future to help the elderly recognise caregivers and visitors, while emotion recognition could be used to detect signs of sadness or depression. All these applications still need the backing of robust scientific evidence before they can be deployed.

While there are no doubt many convenient, new applications, such as face-enabled log-in systems, that are not in themselves problematic, more powerful applications are looming on the horizon and their potential benefits and risks deserve a much closer look. While the use of FR technology for surveillance and law enforcement improves security, the tracking and surveillance of individuals without consent by private parties raises privacy and ethical concerns over the ownership and storage, and use of the images, and could also result in fear and distress. The '10-year challenge' that recently went viral on a number of social media platforms raised the question as to whether the data uploaded were being used to train facial recognition algorithms on age progression and recognition. Sometimes even when consent is given, the purpose for using the technology is not very clear. Applying emotion recognition to hiring and education, etc. could pose high risks, at both individual and societal level. What if algorithms that are meant to help find the candidate best suited to the job actually just perpetuate stereotypes and render a poor service? How can the fair and balanced use of technology be ensured in such cases?

Reports of errors or failures in police use of this technology to identify people shed doubt on the efficacy and purpose of the technology. Reports also show that FR technologies are prone to error when used for datasets of women with dark skin. This kind of bias in algorithms can lead to biased and inaccurate outcomes, with a varying impact on diverse populations and potential implications in the world of work. What can be done to make sure this technology is used fairly? There is a need for policies and regulations to secure the safe and responsible integration of FR technologies and to address the risks posed by blind spots and error. Technology has been shown to be able to detect sexual orientation with higher accuracy than can humans; but research of this kind raises obvious concerns regarding the purposes for which it could be used.

What if some users do not want to give their details or would rather remain anonymous? Can people who do not want their movements tracked for commercial purposes opt out? Could the names of all the entities that collect behavioural biometrics be listed and made publicly available?

Anticipatory policy-making

It is clear that the stakes for FR technology are high in criminal justice, law enforcement, employment, housing, recruitment, health and education. FR is expected to be a booming market in the years to come. An in-depth examination of its potential benefits and risks is essential in order to understand the impact on civil rights and liberties. New regulations must ensure that the algorithms deployed are fair, unbiased and balanced, and the purposes for which they are used is made clear rather than being kept secret. It is also crucial that stakeholders employing FR be held accountable for they ways they collect, use and store data.

Article 6 and Article 9 of the General Data Protection Regulation (GDPR) refer to the consent that an individual must provide before his or her personal data (including biometric data) can be processed for a specific purpose. That consent is one of a number of conditions that must be met if the processing of an individual's data is to be considered legal. Article 32 provides for the protection and error-proof recovery of personal data in the event of a physical or technical incident. Are the provisions of the GDPR enough to address the concerns raised by FR technology?

The first Draft Ethics Guidelines for Trustworthy AI were recently issued by the European Commission's High-Level Expert Group on Artificial Intelligence. They cover issues such as fairness, safety, transparency, the future of work, democracy and, more broadly, the impact on the application of the Charter of Fundamental Rights, including privacy and personal data protection, dignity, consumer protection and non-discrimination. EU law-makers, together with all FR technology stakeholders will need to interact, engage and play an active role to help the Commission to formulate regulations that secure the fair use of this technology.

STOA@ep.europa.eu (contact) http://www.europarl.europa.eu/stoa http://www.europarl.europa.eu/thinktank (internet) http://epthinktank.eu (blog)