Facial recognition and privacy

Facial recognition is becoming widespread and can be used in a range of areas, such as unlocking your smartphone or making payments. The technology is swift, simple and reliable. However, it can also facilitate mass surveillance – without public awareness.

AI is the main driver

Between 2014 and 2018, the success rate for facial recognition systems improved from 96 to 99.8 percent. The technology has become better than humans at recognising faces and is by many considered to be more secure than passwords.

Machine learning accompanied by the vast amounts of photos and videos online contribute to a continuous improvement of the technology. Specialised hardware is not necessary as facial recognition software can be applied to images from most computers, smart phones and digital cameras.

In order for a computer to be used for facial recognition, it must first be able to identify a face in an image. The image can be a photograph or real-time video from a surveillance camera.

Further, the faces are analysed, and a biometric template is created based on the individual's distinct characteristics, such as the distance between eyes, nose and mouth, or other more abstract attributes. The template is subsequently compared to another image or a database of images to verify matches.

SUMMARY

- Facial recognition is a reliable, cheap and effective tool for identification.
- The technology has rapidly developed over the past years and is increasingly used in novel areas. Facial recognition can replace passwords, be used as a means for making payments, access control, and in matters of national security.
- Facial recognition is scalable and enables mass surveillance from a distance, and without consent. Facial recognition is already extensively used in China and in many areas, it is now impossible to be anonymous.
- GDPR regulates the use of facial recognition in Norway, but it is not prohibited. Swedish police recently got approval from the Swedish Data Protection Authority for using the technology.
- Local authorities, technology developers and others are now calling for a moratorium.

Various Types of Facial Recognition

Facial recognition can be used in multiple ways. When the purpose is verification and identification, a face is defined as biometric information.

Verification: Are You Who You Say You Are?

Verification involves comparing two images and determining whether they are of the same person or not. This technology is, for example, used for unlocking smartphones.

Identification: Who Are You?

A picture is compared to a watchlist of images to find a match. These images can come from a variety of sources including photographs and videos from surveillance cameras. The police can use this technology when comparing an image of a person to a watchlist of wanted people.

Another area of use for facial recognition is facial analyses where the algorithm categorises people based on their physical appearance. This is for instance used to generate personalised advertisements, but also by Chinese authorities for ethnic categorisation of the Uighurs, a Muslim minority. Additionally, the technology has been applied in the health sector to help diagnose depression and for remote heart rate tracking.

A Prevalent Technology

Your face is unique and something you always carry with you, and thus facial recognition can reduce the risk of identity theft and prevent sensitive information from going astray. Such solutions are also of practical value to the user as it diminishes the need to remember passwords and codes.

In 2017, Apple launched the iPhone X with Face ID. For the first time users could unlock their phone by merely looking at it. By 2024, facial recognition technology is projected to be included in 90 percent of all smartphones.

Pay with Your Face

In Spain, CaxiaBank has installed ATMs where the PIN number is replaced by facial recognition.

China is investing heavily in financial technology and has adopted a leading position globally. Chinese consumers can already purchase items by showing their face to the camera at the check-out. The ecommerce payment platform Alipay stimulates the technology development by subsidising stores and consumers that are using the technology. In Oslo, TINE SA – one of Norway's largest food companies – and the country's largest bank DNB are currently testing a similar payment solution.

Security and Surveillance

Both private and public actors use facial recognition for security and surveillance. These include firms responsible for security in large arenas and shopping malls, or police and security services.

An international survey shows that actors in 65 countries use facial recognition for surveillance. German train stations are testing facial recognition as a security measure and as a tool for providing support to the police. In January 2020, The Metropolitan Police Service in London announced the introduction of live facial recognition in various public places in the city.

The technology has rapidly spread to an array of countries. Due to the Chinese Government's focus on artificial intelligence and their profuse access to faces, Chinese companies are front-runners in the technology development. Authorities in 52 countries are now using Chinese facial recognition technology.

During the 2020 Olympic Games in Tokyo, checkpoints equipped with facial recognition systems will be used to guide the athletes, staff and media through the various control posts. Facial analyses will also be implemented to help detect irregular behaviour. Heathrow Airport is now testing whether employing facial recognition technology can reduce the time it takes to go through security and check-in, and subsequently improve the flow of passengers through the airport.

Increasingly accessible

As the technology becomes cheaper and more available, new types of services are likely to emerge. Clearview is an app that allows you to take a picture of a person and run it through the company's massive database consisting of more than three billion images. The pictures are collected from open sources on the internet, including Facebook and YouTube.

This suggests that the technology is highly likely to be able to identify a random person on the street. According to the company, the Clearview technology is used by several hundred U.S. police departments and multiple private security companies.

Mass Surveillance

Many of the same qualities that make facial recognition so effective and user-friendly can also facilitate mass surveillance. The technology can be used in real-time, from a distance, and without consent, which makes it hard to detect. Additionally, its immense capacity allows the technology to analyse millions of faces in the blink of an eye.

Facial recognition can thus be a vital tool for authoritarian regimes as it enables constant mass surveillance without public awareness of when or how it happens. Hungarian authorities plan to implement extensive systems for public surveillance through facial recognition to identify criminals. The systems will be used to detect everything from minor traffic violations to matters of national security.

Chinese Dominance

The Chinese Government has employed facial recognition technology in a range of areas. The technology is, for instance, used to identify and shame jaywalkers, and in the police's smart glasses to identify suspects in criminal cases. Furthermore, anyone who wants to apply for new internet or mobile services are required to use facial identification as a means of verifying their identity.

Xinjian, a north-western region in China, was used to test various forms of surveillance. For example, facial recognition has been utilised to track and control the Uighurs. The system identifies Uighurs based on physical characteristics and traces their movements.

The Hong Kong police have had access to facial recognition technology for several years. However, there is a lack of transparency regarding how it is used. The Government has avoided answering questions of whether the technology is used to track Hong Kong protestors. Consequently, the protestors assume they are being monitored and cover themselves with face masks and umbrellas to prevent the cameras from identifying their faces. There have even been instances where protesters have toppled and dismantled smart lampposts due to the looming suspicion that these may be equipped with facial recognition technology.

Risk of Discrimination

Machine learning and algorithms for facial recognition have improved significantly over the past few years, but there are still issues related to the accuracy of the technology.

Varying Conditions

One challenge is whether the technology actually functions as intended. Generally, the algorithms are accurate, but there may be substantial differences in pictures taken in controlled circumstances (such as a police station) and pictures from an outdoor surveillance camera.

For example, a study using facial recognition during the 2017 Champions League final in South Wales showed that as the sun set, the camera failed to recognise faces in the video stream. The algorithm compared the crowd to a police watchlist and misjudged 92 percent of the instances. This illustrates that even tiny disturbances in the video stream can significantly reduce the accuracy of facial recognition.

Discrimination

The quality of the training data sets may pose another challenge. In order to learn what a face is, the algorithms must analyse a lot of images. In 2016, Microsoft created a large database with images of celebrities. The database has been widely used by researchers, private companies and governments. However, the vast majority of these images depict white males, which thwarts the algorithm's accuracy when analysing images of people from other ethnicities, women, or elderly.

This issue can lead to either false positives, where the algorithm incorrectly indicates a match, or false negatives, where the algorithm fails to recognise two images of the same person.

Since the accuracy is largely dependent on a person's physical appearance, it can lead to racial discrimination: Ethnic minorities will frequently be stopped in security controls as they are flagged by the system, or the algorithms may be unable to confirm their identity.

In 2018, the human rights organisation ACLU tested Amazon's facial recognition system. The results revealed a series of false positives. For instance, the system incorrectly matched 28 images of American members of Congress in a database consisting of mugshots. Most of these members were African American.

Regulating Facial Recognition

Facial recognition can be invasive to privacy. Although useful and effective in certain situations, the technology can have significant societal consequences in others. For privacy, anonymity, and protesters, the perils can be far greater than the potential benefits.

The possibility for tracking and identifying people without their involvement or consent is particularly problematic. It violates fundamental human rights, disregards privacy, and can cause a chilling effect where people alter their behaviour due to the suspicion of being watched.

Thus far, there are no known instances where Norwegian authorities have used facial recognition to track or identify people in public.

GDPR and national regulation

Biometric characteristics, such as facial identification, is categorised as sensitive information under the GDPR. This entails strict regulation of how this information can be used.

In 2019, a Swedish school was penalised for using facial recognition to record class attendance. Although the students had provided consent, the Swedish Data Protection Authority concluded that these were invalid since the students are dependent on the school.

However, the GDPR opens for allowing federal authorities to use facial recognition if there is a justified need for it to fulfil their societal responsibilities. For example, in October 2019, the Swedish Data Protection Authority granted the police permission to use facial recognition to identify suspects. This allows the police to compare images with their signalment database, which contains more than 50 000 images. The GDPR demands a Data Protection Impact Assessment (DPIA) to ensure that privacy is upheld. This includes assessing the consequences for basic rights such as freedom of movement without the fear of systematic monitoring.

Call for a Ban

In several countries, both authorities and organisations have advocated prohibiting the use of facial recognition. The hope is that a moratorium makes room for a thorough evaluation of consequences of the technology to establish appropriate measures for a risk evaluation.

In 2019, San Francisco banned the use of facial recognition technology. The reasoning behind the ban is the underlying fear that the technology can be abused, and that even minimal use can contribute to push the U.S. toward becoming a surveillance state. Following the ban, several other cities are barring facial recognition.

The European Commission's white paper on artificial intelligence identifies remote biometric identification, such as facial recognition, as a high-risk application of AI. The Commission plans a broad European debate on what, if any, circumstances that might justify such use. In principle, national authorities must decide whether to allow the technology or not.

Even private companies support a moratorium as it would allow a thorough evaluation of the potential consequences of the technology. Alphabet CEO, Sundar Pichai, publicly announced his support for a moratorium. He maintains that Google do not offer services with facial recognition due to the high risk of abuse of the technology.

Opposing forces argue that a moratorium will inhibit police work and public safety, which impedes technological developments and innovation. The Trump administration wants as little government regulation as possible, but rather place focus on promoting innovation and economic growth.

Authors: Tore Tennøe, Adele Flakke Johannessen and Marianne Barland
Published: Februar 2020, updated March 2020
Contact: post@teknologiradet.no / www.teknologiradet.no

The Norwegian Board of Technology advises the Norwegian Parliament and Government on new technology.