ComputerWeekly.com

How facial recognition technology threatens basic privacy rights

As adoption of facial recognition systems continues to grow worldwide, there is increasing concern that this technology could undermine fundamental privacy rights and how it can be kept in check

Nicholas Fearn

Surveillance and facial recognition technologies have become a common fixture in today's interconnected world over the past few years.

Whether monitoring people in airports, searching for wanted criminals, allowing users to unlock their phones or creating targeted marketing campaigns, adoption of this technology has become widespread and resulted in many useful applications. But it has also generated legitimate concerns around privacy and security.

In December 2018, for example, civil liberties group Big Brother Watch described citizens as "walking ID cards" citing research that found police use of facial recognition tools identified the wrong person nine times out of 10.

As worries that these systems threaten basic human threats to privacy continue to grow, there is increasing pressure on governments and organisations to introduce stricter rules to keep them in check. In May, the city of San Francisco voted to ban police from using facial recognition applications, and California is considering similar moves. Technologists have responded.

Inaccurate tech

Although the use of surveillance and facial recognition technology is widespread and always growing, these systems are still in their infancy and can often be inaccurate. Michael Drury, partner at BCL Solicitors, says the biggest problem is that they are "hit and miss" at best.

"Most people would applaud facial recognition technology if it prevents the commission of terrorist atrocities and other serious crimes. But that remains a very big 'if', and the potential benefits need to be weighed against the cost to us all of having our very beings recorded and those details held by the police," he says.

"We know it is better at recognising men than women, and Caucasians rather than other ethnic groups. The potential for misidentification of suspects and miscarriages of justice is one which should not be underestimated.

"Police and other law enforcement agencies should be wary of seeing new technologies as a panacea and worthy of use simply because the word 'digital' can be used to describe them."

Miju Han, director of product management at HackerOne, echoes similar concerns with regards to the reliability of these systems.

"Facial recognition technology has two major problems," says Han. "The first is that its accuracy is nowhere near 100%, meaning that employing the technology will result in many false positives. Few algorithms were trained on a truly representative sample, so facial recognition will disproportionately negatively affect different demographics.

"But even if we take the highest demographic accuracy today – which is around 99% for white males – and used the technology in a high-traffic area to attempt to identify known terrorists, for example, 1% of all passers-by would be incorrectly tracked, which would quickly add up to hundreds or thousands of errors a day.

"The second major problem is that users have not consented to being scanned. Going out in public cannot be a consent to be tracked. It is possible for an entity to use facial tracking to construct full location histories and profiles, albeit with a lot of errors. Your face is not a license plate."

Harming privacy

When it comes to building a case for surveillance and facial recognition applications, it is often argued that they aid security. Steven Furnell, senior IEEE member and professor of information security at Plymouth University, believes that this can be problematic.

"Security and privacy are often mentioned in the same breath and even treated as somehow synonymous, but this is a very good example of how they can actually work in contradiction," he says. "The use of face recognition in a surveillance context is presented as an attempt to improve security – which, of course, it can do – but is clearly occurring at a potential cost in terms of privacy.

"It has been claimed that face recognition technology is now societally acceptable because people are used to having it on their smartphones. However, the significant difference is that this is by their choice, and to protect their own assets. Plus, depending on the implementation, neither the biometric template nor the later facial samples are leaving their device.

Furnell argues that, in the implementations deployed in public spaces, the subjects are not consenting to the creation of templates nor the capture of samples.

"The data is being used for identification rather than authentication. As such, the nature of the usage is significantly dissimilar to the more readily accepted uses on a personal device," he says.

Comparitech privacy advocate Paul Bischoff says people need a way to opt out and that, without checks and regulation in place, face recognition could quickly get out of hand.

"Face recognition surveillance will probably grow more commonplace, especially in public venues such as transportation hubs and large events," he says.

"It brings up an interesting discussion about the right to privacy and consent: do you have any right to privacy in a public place? Up to now, most people would answer no.

"But consider that even in a public place, you have a certain degree of anonymity in that the vast majority of people do not know who you are – assuming you're not a public figure. You can get on the subway without anyone recognising you. But if a security camera armed with face recognition identifies you, it can tie your physical identity to your digital identity, and it can do so without obtaining your consent first.

"People act differently when they know they're being watched, and they act even more differently if the person watching them knows who they are. This can have a chilling effect on free speech and expression," says Bischoff.

Clamping down

With these threats in mind, some governments and organisations worldwide have begun implementing stricter rules and regulations to ensure such technologies are not abused. More recently, city officials in San Francisco voted eight-to-one to ban law enforcement from using facial recognition tools.

Joe Baguley, vice-president and chief technology officer of Europe, Middle East and Africa (EMEA) at VMware, believes that the city of San Francisco is right to show caution in this case.

As Drury and Han pointed out earlier, Baguley says the problem is that facial recognition software is not yet sophisticated enough to positively benefit police and other public services.

"Its previous use in the UK by South Wales Police, for example, saw 91% of matches subsequently labelled as false positives, which showed the technology does not possess enough intelligence to guarantee accurate results, or to overcome any unconscious bias which may have affected its development," he says.

Before these technologies can effectively assist with policing and surveillance, Baguley says the underpinning artificial intelligence (AI) algorithms need to be altered to ensure the software recognises people without any discriminatory bias.

"Ultimately, we're at a nascent stage of the technology. These issues can be ironed out by enriching it with enough intelligence to make it a sufficiently safe and powerful tool to deploy in the future. It's just not ready yet," he adds.

However, it is not just in the US where legal and regulatory challenges surrounding facial recognition technology are taking place.

In March, the UK's Science and Technology Committee warned that live facial recognition technology should not be deployed by British law enforcement until concerns around its effectiveness were resolved.

In June, a court in Cardiff concluded that rules governing facial recognition systems need to be tightened after a Welsh shopper launched a legal challenge when a South Wales Police camera took a picture of him.

Robert Brown, associate vice-president at Cognizant's Centre for the Future of Work, says these challenges herald a sea change in how much privacy we are willing to give up in the name of safety.
"On the one hand, it is a natural reaction to think, 'Good, facial recognition helped catch a bad guy'," he says. "But then you wonder, 'How often can that 'eye in the sky' see me – and can I trust it?'
"The health of our democracy – and the future of work – demands trust. But the tech trust deficit isn't closing. Too often, there is retroactive *mea culpas* that 'we didn't do enough to prevent X from

happening’. Meanwhile, there is a near-unanimous agreement that facial recognition software error rates – especially among persons of colour – are unacceptably high.”

Brown says that as we continue to see the rise of facial recognition as a means to keep us safe, we are going to have to navigate a thorny mix of standards, laws, regulations and ethics. “This means that we need consent of citizens – not digital-political overlords – to ultimately control who watches the watchers,” he adds.

While many organisations and experts are opposed to mass surveillance, others are more positive. Matthew Aldridge, senior solutions architect at security firm Webroot, sees legitimate applications from law enforcement and other similar agencies where face recognition technology could greatly reduce policing costs and increase the chances of successful prosecutions in certain cases. But he agrees that use of these systems should be limited and regulated.

“In these situations, it should only be perpetrators of crime who have their biometrics stored in this way. There is a temptation in mass surveillance to build a profile on every unique person detected, track their movements and categorise them into behaviour groups,” says Aldridge.

“This type of approach is being taken in China, for example, where the state is able to not only do this, but to map the profiles to the identities of the individual citizens concerned, raising questions about how and why this data is being used.

“Current facial recognition technology can work well, but it is far from perfect. Despite its shortcomings, it demonstrates its value by reducing the workload of investigators, effectively augmenting their role.”

Mitigating the risks

With facial recognition constantly gaining traction for a range of purposes, it is clear that more needs to be done to keep this technology in check.

Chris Lloyd-Jones, product and engineering lead of emerging technology at professional services firm Avanade, believes that current laws need to be revised and that change management is crucial. “As a society, we are not clear around how we handle the limitations of the technology that has the potential to affect emotions and morality – for example, the exceptions and false positives around race and implicit bias, as well as the possibility to entrench biases that already exist in society,” he says. “The legislation in this area does not clarify generally how the technology should be used, and it’s a difficult tool to challenge. If you are walking down the street, and you notice a police CCTV operation, by the time you see the notice, your face is already recorded.

“Change management is important, focusing on handling the exceptions, and empathetically dealing with any false positives that are raised – and feeding this back to the creators of the technology to avoid entrenching existing biases within the technology, such as racial discrimination.”

On a regulatory level, the use of facial recognition tools is already governed by laws such as the General Data Protection Regulation (GDPR).

“Principles such as storage limitation, data minimisation, and lawfulness, fairness and transparency apply to the processing of this data,” says data privacy expert Tim Jackson.

"Additionally, as facial recognition data is a type of biometric data, it can only be processed in restricted circumstances, such as if an individual has given their explicit consent or if a specific scenario under EU member state law has been met."

However, Jackson adds that there is no code of practice that applies to the processing of biometric data. "The Information Commissioner's Office [ICO], as required by the DPA [Data Protection Act], has previously produced codes of practice on other types of processing such as direct marketing and subject access, and has recently published a draft code of practice regarding children's online privacy," he says. "It has also closed a 'call for views' consultation period with the intention of producing a code of practice on how to balance data protection in journalism. I would therefore expect the ICO – when formally instructed by the home secretary – to lead the way with a biometric data code of practice in the near future."

Despite the lack of a specific code of practice, there are a number of steps that need to be taken by companies that are developing or using this software.

"As we are talking about a high-risk processing activity, a data protection impact assessment must be carried out before the processing begins," says Jackson, adding that the ICO provides detailed guidance on what form this assessment should take.

"This assessment will help the company identify the various risks that need to be mitigated, risks such as discrimination, unconscious bias, lack of transparency, and lack of proportionality, for example." Jackson recommends ensuring that the development stage of any facial recognition software includes representation from different ethnicities and genders; ensuring individuals whose data are to be processed are made fully aware of this activity, what rights they have in relation to their data, and how to invoke these rights.

He adds that it should also apply strict retention periods to the collection of any data; apply confidentiality measures to the collection of any data; consider whether the scope of the facial recognition software could be reduced; seek the views of individuals before the processing begins to understand their concerns and adopt further measures if necessary.

Any facial recognition system should also consider whether there are alternative, less intrusive ways to achieve the same outcome; and create policies to govern the processing activity and to provide direction to staff, according to Jackson.

It seems the use of facial recognition technology is a double-edged sword. Although some people argue that these systems play an important role in fighting crime and assisting with other important tasks, they also present privacy challenges and risks.

As adoption increases, safeguards, laws and regulations will certainly need to be reviewed and revised to ensure consumers are protected and that this technology is not abused.

It is therefore no surprise that the UK surveillance camera commissioner Tony Porter is calling for a strengthening of the code of practice for the surveillance camera industry in the face of new privacy regulation and surveillance technologies such as facial recognition.

The online link to the article can be found here.