Totalitarianism with a human face: The combination of surveillance cameras and face-recognition software is creating new threats to such freedoms as remain

Sam DeSilva

Reprinted from *Arena Magazine* (4/1/02) with appreciation

June 18 1999 was an international day of action against corporate globalisation that focused on the G8 summit held in Cologne, Germany. Protests occurred in over forty countries, but activists from London got the most attention, where actions were claimed to have caused `massive criminal damage' costing the city over 2 million pounds.

Following the J18 protests, police cut faces from video and photo surveillance and uploaded them on to the City of London website. `Your help is needed to identify and locate the suspects depicted in the photographs on the following web pages', requested the site.

There is nothing new about the authorities using surveillance during protests, but J18 was the first time that faces of protestors had been lined up on a website and the public's assistance requested with identification and location.

After September 11, the faces of the nineteen `terrorists' were exposed to the world. The global media networks implored: if these faces had been prevented from boarding those fateful flights, could the destruction and loss of life have been avoided?

The providers of facial analysis systems seem to think so. The `face-cam' is the media buzzword for this technology. It is a surveillance system that incorporates the camera with computer software and a database of facial images of `wanted' criminals. The camera captures an image of a scene of people and the software extracts any faces captured in the video frame. It then does a comparison against the database of criminal faces. If there is a match, alarm bells start ringing.

The businesses peddling these systems insist they work. Already, some airports in the US have installed face-cams. Visionics Corporation provides technology solutions for `Human ID at a Distance', which their website claims `will automatically capture faces in the field of view, extract them from their background and compare them against a watch list or database of certain individuals'.

Common sense makes us question the accuracy of such systems. Can a surveillance camera record a precise image of a face that may be obscured by hair, a hat or sunglasses?

There has been a concerted effort recently to develop automated facial analysis systems that are accurate. The `Face Group' researching out of the Robotics Institute at Carnegie Mellon, is investigating various strategies to analyse facial expressions and recognise faces. The facial expression analysis is based on a face language, which assumes that the way we smile and scowl is hardwired. The recognition is also based on fixed data and works by comparing appearance or the geometry of the face with stored information.

The Facial Action Coding System, or FACS, is primarily the brainchild of academic Paul Ekman. FACS works on the premise that it is possible to use a formula to recognise facial expressions, even from faces belonging to different cultures.

In March of 1999, the Salk Institute for Biological Studies distributed a press release titled `Computer Program Trained to Read Faces'. Ekman and his FACS are integral to this project, which has attempted to develop an automated facial analysis system. Though not yet perfected, Salk claims that their software could efficiently analyse the micro-expressions on people's faces, which often expose their `insincere emotions'. Law-enforcement agencies are interested in the technology which, according to a recent email from Salk, `is still being developed and is not used for any practical application at this time'.

In January 2001, for the SuperBowl in Tampa, Florida, a number of companies specialising in surveillance and facial analysis products teamed up with local law enforcement agencies to showcase a system that claims to pick out `mischief, criminal behavior and larger threats'. As fans walked into the stadium, cameras captured their faces and compared them with a database of faces of known criminals.

Predictably, many civil rights and privacy advocates were outraged. A strongly worded statement released by the American Civil Liberties Union (ACLU) of Florida questioned whether the general public should be subjected to the `computerized police line-up' and asked what would happen to the captured images.

One way for the government to satisfy the privacy and civil liberties concern is to ensure a higher level of accountability and transparency through legislation. This is happening in many countries. As of mid-December 2001, Australia's Privacy Act applies to the private sector as well as to public organisations and, according to the Federal Office of the Privacy Commissioner, facial images captured and stored by surveillance cameras form a `personal record' which is covered by the Act. Agencies involved with facial analysis are therefore required to `advise people of the identity of the collecting organisation that they are collecting the information for, what the information will be used for, who they disclose the information to, and how the individual can access the records the organisation holds about it'.

Rather than arguing against the deployment of the face-cam throughout our cities, government legislation can help further legitimise its use. And as corporate interests and `security threats' increasingly influence government policy, exceptions will creep into the rules. Initially, face-cams may look out for a small number of known terrorists; but over time the role of the system could expand to keeping tabs on many categories of people.

Following September 11, support for face-cam technology increased significantly. In the following month, a number of airports in the US announced that they would install software to automate the process of excluding known suspects. But, like in the SuperBowl case in Florida, there has been strong opposition. The ACLU spoke out again, this time releasing a detailed report on why face-cam technologies should not be used. Other than the privacy issues, the report cites a US Department of Defense study which `found

very high error rates even under ideal conditions, where the subject is staring directly into the camera under bright lights'.

But when the majority of the public seemed to have swallowed the `war on terrorism' line, there is little reason for governments to consider what groups like the ACLU have to say.

Face-cams have been installed in some cities for many years. Casinos have also been using the system to exclude known cheats and punters who never lose. The first city to utilise face-cams was the London Borough of Newham, which had technology by Visionics Corporation installed in late 1998. The system utilises visual information from a network of over 140 surveillance cameras to identify `target faces'.

But a recent article from CBS News indicates that the technology can be tricked. When a clear shot of the `target' is presented, the system makes a match; but it fails when `a cap and sunglasses' are worn. In the article, privacy advocate Simon Davies suggests that surveillance `makes people behave differently ... It makes them cautious, neurotic. It changes their interactions. Everybody is brought to heel. Everybody's made to be good. It's like living in some giant shopping mall'.

David Lyon's `Surveillance Society: Monitoring Everyday Life' comprehensively explores the issues surrounding surveillance and provides fresh insights into the issues which go beyond the privacy and the `civil liberties discourse'. Lyon refers to a number of major themes in his book, including the idea that surveillance is an essential tool for evaluating and managing risk.

Face-cam surveillance claims to deliver identities at a distance, or in other words, the technology claims to be able to identify someone without their knowledge. These automatic systems could prevent people who displayed similar features to suspected criminals from crossing borders. The technology could also be used by insurance companies and marketers to optimise their practices.

As face-cam technology becomes widely utilised, its cost will go down. Local convenience stores to stock exchanges may exclude people based on face-cam analysis results. If face-cams have the ability to isolate faces from a city streetscape and store that information in a database, it would not be too difficult to construct databases of faces sorted according to where people live or spend a majority of their time. An up-market shopping centre might then, as an example, exclude or at least alert security when faces from a poorer part of the city tried to enter.

These are simply scenarios and could be dismissed as paranoia. But one of the aims of this article is to provoke thought around the subject of surveillance and to further investigate how it could be applied in future contexts. For example, what impact might face-cam technology have on civil disobedience?

While the freedom to assemble and protest is supposedly our democratic right, many of the recent protests in Melbourne, Australia have had official non-uniformed camera crews filming the people. This is most likely the same elsewhere and it certainly was the case during J18 in London. It would not be difficult for facial analysis to be applied to protest footage, enabling the recognition of `regular' faces. Though the accuracy of such analysis is under question, authorities could claim to identify ringleaders. Faces of protestors could be packaged on to DVDs or made available through the internet to potential employers. People would certainly think twice before attending protests if they knew face-cams would be in operation.

The scenarios above consider facial analysis technology in terms of recognising faces. But if Paul Ekman's FACS is incorporated into face-cams, could authorities then claim the ability to determine

motivations and thought patterns by evaluating expressions?

There is evidence to suggest that face-cam technology is far from perfect; and commonsense should tell us to be wary of a facial language that claims to be able to decipher our emotions. We also need to question the integrity of the database itself, and consider that facial analysis reinforces the idea that it is acceptable to judge someone by the way they look.

Sam de Silva is a Melbourne-based media-maker. sam@myspinach.org