FACE UP TO IT!

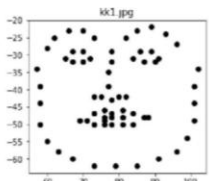
Facial recognition and Artificial Intelligence are here and now – and so are the ethical questions associated with these technologies.

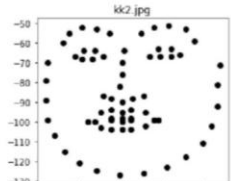
Biometric Artificial Intelligence systems try to uniquely identify a person by analysing patterns based on facial textures and shape. There is increasing use and coordination of IT, AI, CCTV, big data, IoT and GPS systems to spot individuals and groups of people, to track their locations and movements, and even to deduce their intentions.

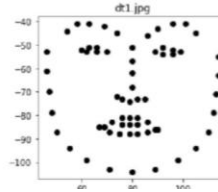
But as yet, mechanisms and assumptions are often inadequate or incorrect – and lead to significant ethical issues, as well as legal, privacy and other questions.

At a recent event at BCS (British Computer Society) in central London, Kamal Khan (Director of ISACA London Chapter) gave an overview of how facial recognition works, increasing use of new technologies, and the growing concerns and issues coming into focus.







Above: two images of Kamal Khan and one of a well-known personality you may recognise.

Question: How does Facial Recognition work?

1. Your picture is taken.
2. FR software reads the geometrical parameters of your face.
3. Your facial signature is compared to databases of known faces.
4. A determination is made if your facial signature matches that of an existing image in an FR database.

Question: Is my face being stored in databases?

Kamal reassured us that a standard image as we know it is not stored.
Although a photograph of a face is initially taken it is then run through software that creates dimensions or geometry, which in turn is translated into a complex algorithm. It is this

algorithm that is stored and which may be used to compare with others to trace a match if necessary.

Recent news about use of facial recognition systems

- The Australian government has proposed using a facial recognition system to verify that people who seek to watch pornography online are of legal age.
- Sweden's data protection authority has approved the use of facial recognition technology by the police, to help identify criminal suspects.
- A growing number of American cities are debating the use of facial recognition systems.
- In the US, security services at airports can automatically flag up those on no-fly lists.
- The Beijing subway system will apply facial recognition technology to passenger security checks to improve transport efficiency.
- Researchers in China have developed an ultra-powerful camera capable of identifying a single person among stadium crowds of tens of thousands of people.
- China is now exporting its model of surveillance around the world, offering trainings, seminars and study trips, as well as advanced equipment that takes advantage of AI and facial recognition technologies.

Question: What security and ethical issues can arise from misuse of facial recognition data?

- At an Individual level: Data privacy, bullying, downloading copyright material without permission, unfair bias based on individuals' race or sex.
- At a Corporate level: Misuse of data; excessive monitoring, profiting from personal data without permission.
- At national/international levels: Cyberwarfare, mass surveillance; and of course 'Fake News'!

Question: How can we address these and other issues?

A number of courses of action were discussed at this lively and interesting BCS event.

What do you think?

Want to see the video, and more 'hot topics' hosted at events by the dynamic North London Branch of BCS – The Chartered Institute for IT?
Go to www.nlondon.bcs.org 'Past Events' or directly to https://nlondon.bcs.org/pe/pe2019dec11.htm

Written by Dalim Basu, Chairman of North London Branch and London Central Branch at BCS – The Chartered Institute for IT