

Smart CCTV

Prof. Simon Rogerson

**Originally published as ETHicol in the IMIS Journal Volume 12
No 1 (February 2002)**

Surveillance has become part of everyday life. The compelling arguments for its introduction into public spaces as means of ensuring public safety have led to CCTV cameras perched high above every street corner within towns and cities. The next generation of surveillance, smart CCTV is now being introduced under the guise of routine maintenance and upgrade. In June 2001 100,000 people attending the Super Bowl in Florida had their faces scanned in search of wanted criminals.

Smart CCTV is the combination of video surveillance with facial recognition technology and is used for face finding, face recognition and face tracking. Advances in facial recognition technology, using faceprints based on facial geometry, has been significant. According to Visionics Corporation, it is now possible to search one million faceprints per second with an error rate of less than one percent. Contextual factors such as lighting, expression and profile have no real impact if the image is of good quality.

Philip Brey of the University of Twente in the Netherlands discussed the ethical issues of smart CCTV in public spaces in a paper he presented at the CEPE conference held at Lancaster University in December 2001.

He reports that in the UK smart CCTV has been used in the London Borough of Newham since 1998. At the time the following was reported in Computer Weekly (13 October 1998):

"The London Borough of Newham aims to cut crime by 10% within six months by using face recognition software to pinpoint criminals on CCTV cameras. The pilot, to be jointly launched tomorrow with the Metropolitan Police, is the first local authority implementation of the technology.

Newham has already fielded enquiries from 20 councils and eight police forces, and Bob Lack, Newham's emergency services manager, predicted that many of the 250 councils in the CCTV user group would soon adopt the technology. But the project has drawn criticism from the Data Protection Registrar, which has voiced concern over the implications for privacy.

The Registrar is seeking a meeting with the Metropolitan Police. "People are being compared to convicted felons - there are clear civil liberties implications," said Jonathan Bamford, Assistant Data Protection Registrar."

In 2001 the Newham system was linked to a central control room operated by the London Metropolitan Police Force. In April 2001 the existing CCTV system in

Birmingham city centre was upgraded to smart CCTV. People are routinely scanned by both systems and have their faces checked against the police databases.

Brey explains that the debate about smart CCTV has primarily centred around the security benefits of the technology versus the threat to privacy and freedom. He points out that it is vital to understand thoroughly the tradeoffs that have to be made between security and civil liberties when considering how and where to use smart CCTV. "A better understanding is needed of both the importance of civil liberties and the importance of security, of power and reliability of the technology, and of its potential uses and abuses." Brey identifies three ethically charged problems associated with smart CCTV.

Error

This is where incorrect matches result in innocent people being subjected to investigation and harassment by the police. Brey suggests that "this problem does not in itself present a strong argument against smart CCTV. It only suggests that every care should be taken to minimise error, to minimise the inconvenience to mistakenly identified citizens, and to evaluate whether the tradeoffs that are made are still reasonable."

Function Creep

This is where the purpose for using smart CCTV may be easily extended from identifying criminals and missing persons to include other purposes. This could occur by widening the faceprint database to include, for example digitised images from driving licences. It could occur by undertaking analysis of crowd behaviour and membership or tracking individuals over a period of time to ascertain movement and interaction behaviour. It could occur by the system being used by new types of users for example international law enforcement agencies or local town councils. Individual operators could use, albeit unauthorised, the system for their own purposes. Brey argues that unacceptable function creep is a common problem with all new technologies and cannot be wholly avoided by regulation. He suggests that there is "an obligation on developers and users of technology, therefore, to anticipate function creep and to take steps to prevent undesirable forms of function creep from occurring."

Privacy

Intrusions on privacy through observation of individual behaviour is a common problem with all surveillance. Smart CCTV suffers from an additional problem. The face is a 'highly personal aspect of one's body' and smart CCTV captures this in

digital form as a faceprint. Brey points out that in this context the face is nothing more than an information structure. He explains that "the unique features of one's face, by which others recognise you and which help to define your uniqueness, can be encoded into a computer file of only 88 bytes. This functional reduction of body parts to information structures is one that many people find dehumanising." He points out that "the faceprint that uniquely characterises your face is not 'yours' but 'theirs': it is not owned by you or even if it were, it would not be understood by you because you do not understand the technology." Thus smart CCTV pose two privacy problems.

Whilst smart CCTV does provide social benefit it does require a reduction in civil liberty. People do have justifiable privacy expectations even when they are in public space. Such expectation can be violated by smart CCTV. Furthermore faceprints are part of our electronic persona and as such must be treated as part of us. It is unlikely that developers or those applying this technology have considered such issues in depth. The call must be for an effective social audit process when such technological applications are being considered. This process should capture and take into account the opinion of those directly and indirectly affected.

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson
Director
Centre for Computing and Social Responsibility
Faculty of Computing Sciences and Engineering
De Montfort University
The Gateway
Leicester
LE1 9BH
Tel:(+44) 116 257 7475
Fax:(+44) 116 207 8159
Email:<srog@dmu.ac.uk>
Home Page: (<http://www.ccsr.cse.dmu.ac.uk>)