Automatic Face Identification – Privacy and Security against Crime
Michael Bromby - Division of Law, Glasgow Caledonian University

Abstract
Computerised, automatic face identification and recognition systems have advanced during the past decade. The current focus on crimes such as terrorism, illegal immigration and identity fraud/theft has increased the relevance and application of face identification technology.

Involuntary mass surveillance not only raises issues of privacy, but the introduction of collated databanks of images, such as the Driver and Vehicle Licensing Agency (DVLA) database or the proposed Identity Cards Bill\(^1\) progressing through the UK parliament, increases the potential of the technology.

The advances in face recognition software do not remove the problems of mistaken identity, so commonly associated with human visual perception. The perceived accuracy of automated systems can create a false surety of accuracy and reliability. One argument is that the technology only automates the detection of what is easily observable by a law enforcement officer,\(^2\) however, the globalisation of detection, transaction and storage presents new problems.

In the US, constitutional law (the Fourth and Fifth Amendments, which protect against unreasonable searches and seizures and self-incrimination) could regulate the extent to which mass societal surveillance extends and invades public privacy. This, however, only extends to state or governmental surveillance and would not protect against private sector surveillance.

Attempt have been made to preserve privacy by de-identifying facial images\(^3\) by replacing the traditional form of anonymising (pixelation or blurring) with a method to confound algorithms still capable of performing face recognition tasks. These studies will be assessed to examine whether the trade-off between privacy and security can indeed be adequately balanced.

---

\(^1\) HL Bill 55 2005-06; http://www.publications.parliament.uk/pa/ld200506/ldbills/028/2006028.htm