Surveillance & Society
5(1): 33-50
http://www.surveillance-and-society.org

CCTV Identity Management and Implications for Criminal Justice: some considerations*

Moira Carroll-Mayer, Ben Fairweather and Bernd Carsten Stahl[1]

Abstract

The UK Presidency of the European Union called for an expansive, mandatory policy of surveillance technologies aimed at the reduction of crime and the protection of citizens. Research indicates that the efficacy for this task of the technology, epitomised by CCTV, cannot be taken for granted. This paper asks whether the effects of the technological surveillance environment may be more problematic than currently posited in the literature to the extent that they render more vulnerable and undermine the identities of those they are pledged to safeguard. Much of the literature in surveillance studies debates whether surveillance technology, particularly CCTV, has the effects of crime reduction and prevention attributed to it by proponents. This paper goes one step further and through a process of critical analysis explores the import for individuals subjected to the process of surveillance technologies epitomized by CCTV. In particular the paper addresses the question as it is perceived through the postmodernist agenda. Accordingly in the process of critical analysis the paper considers the effects of transcarceration, the phenetic fix and the technological imperative.

Background Issues

McCahill and Norris (2002) estimated that in the UK there are over 4.2 million CCTV cameras, one for every 14 citizens. A UK citizen may be captured on CCTV up to 300 times each day (Murakami Wood *et al.*, 2006: 7). The figures indicate a higher camera/citizen ratio in the UK than in any other state on earth. It is against this backdrop that on the 7th September 2005 the UK Presidency of the European Union released a first formal report on security enhancement entitled *Liberty and Security: Striking the Right Balance*[2]. The main intention of the report was to further promote surveillance technologies in order to safeguard freedom and security. Some of the policies suggested in the report are domestic UK policies that had failed in the UK for a variety of reasons

* In the context of this paper identity management describes the process whereby the individual's identity is recast through the medium of CCTV surveillance technologies.

[1] All: Centre for Computing and Social Responsibility, Faculty of Computing Sciences and Engineering, De Montfort University, UK. mailto:moiracaroll2000@yahoo.co.uk

[2] The report may be accessed at http://www.privacyinternational.org/issues/terrorism/library/ukpresidencypaperonstrikingtherightbalance.pdf. It is also accessible at: http://www.fco.gov.uk/Files/kfile/LibertySecurity.pdf [Last accessed Jan 18th, 2008].

 ISSN: 1477-7487

(Riley, 2003:16; FIPR, 2003). What is nevertheless interesting about the report is that it suggests that surveillance technologies are generally justified in the fight against crime and terrorism. It is based on strong assumptions about the nature of crime, of law enforcement and of the role of technology as a facilitating factor for providing security. But it must be emphasised that there is no agreement as to the effectiveness of CCTV technology as a panacea to misbehaviour. This will come as no surprise to scholars in the field of surveillance studies. Research on the effectiveness and efficiency of surveillance technologies in the UK has shown that their efficacy is dubious. A leading study conducted for the Home Office concludes that CCTV does not lead to crime reduction (Gill and Spriggs, 2005: 60). Gerrard *et al.* (2007:11) are careful to stress the ongoing debate as to CCTV efficacy in crime reduction and prevention. Any analysis of the value to society of increased technologically enabled surveillance must, in the face of its promotion by the authorities as a general panacea, take account of the doubtful status of CCTV as a crime reduction tool.

This paper aims to counter balance the blanket approval of CCTV surveillance technologies by policy makers. Overall, the paper asks readers to go beyond the standard issue of usefulness of CCTV surveillance technology and develop a broader account that allows an appreciation of unexpected and counter-intuitive effects of the technology.

The paper critically analyses the events surrounding the deaths of Rigoberto Alpizar and Jean Charles De Menezes in the CCTV rich environments of an airport and underground rail station respectively. Of airports Adey (2004:1477) has this to say 'they are symbols of mobility, emblematic of the postmodern world… well and truly a space under surveillance'. Since mobility is often viewed as a risk to the social order (Adey, 2004: 1478), it is no surprise that surveillance in the form of CCTV should be concentrated and implicated there in societal conflict. Their role in surveillance has gone largely unnoticed by surveillance studies, reflecting the invisibility of these transient 'non-places' within the social sciences (Adey, 2004:1). Cwerner (2006) concurs and explains, 'the social sciences and humanities have had relatively little to say about these systems and processes (comprising airports) partly because such time-systems are gated and off-limits'. (The position is exacerbated since as Gerrard *et al.* (2007:28) note there is refusal to reveal 'the needs' of state agencies regarding viewing, analysis and recovery of CCTV footage due to national security considerations.) The role of surveillance at airports, largely ignored, reflects that invisibility. Despite invisibility and obfuscation, what happens there [and surely now at rail stations] is a microcosm of events to come as through surveillance technologies a range of political agendas and aspirations strive to effect wider society (Lyon, 2003: 410). We may learn useful lessons from what happens within them for other places and spaces.

The thrust of the paper is all the more pertinent in light of recent research for the Home Office and other major stakeholders in CCTV (Camerwatch Launch Report, 2007) revealing that over 90% of the CCTV cameras from which police evidence is obtained fail to meet the Information Commissioner's Code of Practice and are operated illegally (Ferrie, 2007). Ferrie states too,

> I'm not surprised there is confusion [about CCTV evidence]. It's a complex area…the Data Protection Act covers images of people and

> requires they be held securely if the data is to be used as legal and admissible evidence. Storing images of people is also impacted by the EU Human Rights Act. As things stand today clever legal counsel could drive a horse and cart through most CCTV evidence and that is not in anybody's best interests.

Courts are also taxed by questions of image quality. Cunningham (2007) representing the Home Office and ACPO states 'The use of CCTV as an evidential tool has grown significantly but 89% of CCTV images that reach the police is far from ideal.' The theme is repeated in the National CCTV Strategy 2007,

> Anecdotal evidence suggests that over 8o% of the CCTV footage supplied to the police is far from ideal, especially if it is being used for primary identification or identities are unknown and identification is being sought, for instance by media release.
>
> (National CCTV Strategy, 2007: 2.2.2)

Underscoring these problems are the informing instructions issued by the Fifth Report of the House of Lords Science and Technology Select Committee[3] whereby it is left to the discretion of the courts whether to admit CCTV evidence. Current practice is to admit such evidence even where there are weaknesses arising for example from image quality or authenticity. Such issues go instead to the weight afforded to the CCTV evidence within the judicial process. The Committee having looked at issues effecting the admissibility of digital imaging for evidential purposes for example loss of quality attendant upon compression, image manipulation and authentication concluded, 'Evidence should not necessarily be inadmissible because it does not conform with some specific technological requirement.'[4]. The laissez faire approach is perhaps understandable if it understood, for example, that though it is possible to go through CCTV operating code line by line it is not possible to see it in operation; CCTV software algorithms are operationally obscure (Introna and Wood, 2004:183). This difficulty is equalled by there being a mere handful of experts worldwide with the ability to understand and interpret the algorithmic trial left by smart CCTV (Philips *et al.*, 2003).

Methodology

The paper addresses the issue of CCTV and its implications for identity management within the criminal justice system through the lens of critical theory, it proceeds upon the basis that there is inherent structural conflict at the nexus of the technology and the interests of societal stakeholders. Since the presence of structural conflict provides the ideal milieu for critical research (Fay, 1987: 27) this was a major factor in the decision to proceed from that theoretical standpoint. Taking into account the blanket and pervasive nature of the hegemonic discourse, characterised by the call of the UK Presidency of the EU to intensify CCTV surveillance technologies, a theoretical approach was required that would effectively probe the attendant incomplete, ambiguous and contradictory discourse. Critical analysis finds what lurks behind and what is really being said (Bondarauk and

[3] The full report is available at http://www.parliament.the-stationery-office.co.uk/pa/ld1999798/ldselect/ldctech/064v/st0501.htm

[4] House of Lords Select Committee on Science and Technology Report of 1998, para 3.18 of note 8.

Hubb, 2003: 2). Overarching all of this is the consideration that of all the main stream methodologies only critical analysis permits the identification, investigation and judgement of the effects of phenomenon outside the boundaries of origin. It answers the question 'how' invites prescription and does not preclude dismay (Potter, 1996:3).

Manipulation and Misuse of CCTV Evidence

Gerrard *et al.* (2007: 24) opine, 'there appears little doubt the police service utilizes CCTV images in the investigative process and has considerable success in doing so. High profile cases have reinforced the investigative benefits of CCTV, which not only assist police officers in the identification of offenders but also help establish the nature, location and time of the crime...' Their remark is immediately preceded by an acknowledgement that there is a lack of formal research evidence for the conclusion[5].

It is instructive to look at formal research evidence that does exist. There is near consensus that the presence of CCTV in the working environment of police officers can produce negative effects on their behaviour (Werrett, 2003: 192). These effects may manifest in mistakes or in the commission of criminal offences. Goold (2003) found that though officers positively modify their behaviour in the presence of CCTV that they exhibit a tendency to manipulate CCTV deployment to their advantage. Goold (2003: 199) cites Norris and Armstrong (1999: 190) who identified police practices such as signalling operators to pan away from questionable police activities and ignoring or suppressing CCTV footage in order to create evidential biases. Goold's findings,

> gave reason to believe that police officers at some of the [CCTV] schemes had attempted to remove tapes that they feared might contain footage of police misconduct. At police led schemes operators claimed that on a number of occasions officers had come up to the CCTV control room following incidents in which they had been required to use force and had asked to 'check the tape.'
>
> (Goold, 2003: 199)

According to one CCTV operator interviewed by Goold many officers did not view themselves bound by the Code of Practice rules on CCTV evidence handling and access. Goold reports that officers at police led schemes viewed the evidence as existing primarily for their benefit and displayed signs of regarding themselves as the rightful owners of all evidence generated by CCTV. At times they were emboldened to remove tapes without authorisation.

The proprietary stance of the police towards CCTV evidence must be viewed against the

[5] Gerrard *et al.* (2007:26) report that the Police Standards Unit does not publish performance data for CCTV evidence and that there is therefore no quantifiable data regarding the success of CCTV evidence an investigative tool. The explanation rendered is the absence of all activities relating to CCTV evidence from the police National Competency Framework and that therefore the retrieval and compilation of CCTV evidence is still not a recognised practice or a recognised police officer's role.

'broad concern' regarding the problem of police perjury[6] and police involvement in perverting the course of justice[7] in the UK referred to by Edwards (2002: 1).

Of course the manipulation of CCTV evidence is not peculiar to the police. The Rodney King case is the most compelling extant illustration of CCTV manipulation by both sides in criminal proceedings. In 1992 Mr Rodney King, an Afro-American, was stopped for speeding and subsequently assaulted by the four arresting white police officers. The event was video recorded by a man from a nearby building which recording became subject to various forms of distortion by the opposing sides in the prosecution of Mr King's attackers. Goodwin (1994: 2) states,

Opposing sides in the case used murky pixels of the same television image to display to the jury incommensurate events: a brutal savage beating of a man lying helpless on the ground versus careful police response to a dangerous 'PCP- crazed giant' who was argued to be in control of the situation. By deploying an array of discursive practices including talk, ethnography, category systems articulated by expert witnesses, and various ways of highlighting images provided by the video tape, lawyers for both sides were able to structure [the depicted actions ergo the characters of the actors] in ways that suited their own distinctive agendas…

Though a full consideration of Goodwin's findings is precluded here it is instructive to present from each side an adapted illustration of the many techniques of CCTV evidence manipulation that his research discovered. During the first trial the prosecution presented the recording as self explicating, objective record in these terms, 'What more could you ask for? You have the video tape that shows objectively, without bias, impartially what happened that night. It can't be rebutted' (Goodwin, 1994: 15). Using the same images an expert witness for the defence filtered the taped events through a police coding scheme, instructing the jury to view the victim's body movement in terms of that scheme. A coding scheme for the use of violence was applied to the taped images:

- If a suspect is aggressive the proper police response is force escalation in order to subdue.
- When the suspect cooperates then the force is de-escalated.

Following the application of the code to the images what is in fact a brutal assault is deconstructed into a new set of events as follows:

---

[6] The Perjury Act 1911, section 1 provides for the offence of lying on oath. Lying on oath includes false declarations per the Criminal Justice Act 1967, s.89 and the Magistrates Court Act 1980, s.106 covering statements tendered in committal proceedings and representations punishable under any statute in judicial proceedings. The offence is triable on indictment only and attracts a seven year maximum sentence.

[7] Perverting the course of justice is a common law offence; triable on indictment only it may attract a life sentence though in practice is unlikely to result in a sentence exceeding ten years imprisonment. The offence includes fabrication or disposal of evidence or inducing others to do so. Edwards (2002) indicates that police officers found guilty of perverting the course of justice are likely to attract sentences of between four and seven years for perjury relating to the most serious charges of murder, violence and drugs. Perjury and perverting the course of justice strike at the basis of the rule of law and have been said to 'poison the well of justice' Crabtree J. in R v. Archer, unreported 2002, Para 63.

> Defense: There were ten distinct uses of force rather than one single use of force. In each of those, uses of force there was an escalation and a de escalation an assessment period, and then an escalation and a deescalation again. And another assessment period.

Actions the prosecution describe in the second trial as 'beating the suspect into submission' is then transformed into a display that the 'period of de escalation has ceased':

> Defense: Four oh five, oh one [blows] We see a blow being delivered. Is that correct?
> Expert: That's correct. The force has been again escalated to the level it had been previously, and deescalation has ceased.
> Defense: And at - at this point which is… We see a blow being struck and thus the end of the period of deescalation? Is that correct Captain?
> Expert: That's correct. Force has now been elevated to the previous level, after this period of de escalation.
>
> (Goodwin, 1994: 17)

Goodwin anticipates objections that the expert's point is tautology; that if one is being struck repeatedly then by definition the moments in between are de-escalations. Goodwin responds 'However much more than tautology is involved. By deploying the escalation-de escalation framework the expert has provided a coding scheme that transforms the actions being coded into displays of careful, systematic police craftwork'. At another stage the defence expert codifies images of Mr King's buttocks rising slightly in a manner that unleashes a cascade of perceptual inferences that have the effect of exonerating the officers and of recasting the identity of the victim as the controller of the action (Goodwin, 1994: 22).

The Process of Transcarceration in the CCTV Environment

There are other more insidious forces at work in the CCTV environment. Towards an explanation of the origins and effects of CCTV identity management exemplified at its most extreme by the cases of De Menezes and Alpizar, this paper draws attention to similarities between the characterisation of 'suspects' on CCTV and the characterisation of the mentally ill on televised media through a process of transcarceration. The concept of transcarceration originally described confinement of the mental patient within and between environments wherein the individual's identity and autonomy might be expunged or modified. The concept has been extended by Arrigo *et al.* (2005), Lowman *et al.* (1987) and Haggerty (2004) to cover those targeted by the criminal justice system. Haggerty (2004: 218) describes how environments conducive to transcarceration evolve from the replacement of 'criminological experts who targeted policy intervention at the level of the individual or the social by new experts *in the situational'* [italics added]. Their focus is upon crime control through transformation of the immediate physical environment. Situational criminology stresses crime reduction through loss prevention, target hardening and enhanced visibility; each of these is realised through CCTV as in the

process of transcarceration it reaches out to and is entered by 'suspect' yet silenced individuals. In such a setting the sense making speech is located in the unconsciousness of the viewer 'awaiting mobilization and valorization' (Arrigo *et al.*, 2005).

There are two intersecting axes that pass through the speaking subject (Chong *et al.*, 2006), *the plane of meaning and being* and *the plane of the existential and the symbolic*. The former is identifiable in the linguistic struggle of the psychiatric patient as he seeks to assert his legitimacy through the limiting, established clinico-legal system of communication. The latter is identifiable in the articulation of self referential, thematic, circulated meanings and values of the clinico-legal professions. Clinico-legal speech, the medium for discussion of mental illness, is 'steeped in and governed by a grammar that privileges disciplinary systems' (Foucault, 1977). In the taken-for-granted clinico-legal communication setting the mentally ill are over time denied the individuality and validity they would otherwise posses.

Consider now the societal response to one whose likeness appears on CCTV footage that has been sequestered or otherwise obtained for the identification of a criminal actor. Not for him a luxurious world where disempowered voices may nonetheless be heard from 'the plane of meaning and being' (Chong *et al*., 2005). In the silent movie world of CCTV evidence, in a process of 'transcarceration' (Arrigo *et al.*, 2005), suspects are moved between nowhere and the scene of crime. Worse, they are left hovering, loitering at the scene, assuming guilt by association. Separated from reality, isolated in virtual reality, deconstructed within hours, minutes or seconds, according to the temporal constraints of pressurised police activity, they have *no voice*. This is, as Chong *et al.* (2006) would have it, the 'manifestation of punishment assuming a discursive linguistic form'. The superimposition of the suspect's silence by the voice of authority has consequences that will be considered.

Personal appearances upon publicly located CCTV screens are unaccompanied by the voice of the actor. They acquire, in the hands of the police however, a 'voice over'. The absence of voice is important in the process of transcarceration. The superimposition of the voice of authority is critical. From this side, through the lens of critical postmodernism, it is possible to explain how the superimposition of the voice can lead to the virtual criminalisation of those depicted on CCTV. It partially explains the horrifying consequences, for Jean Charles De Menezes, attendant upon the appearance of his look-alike, a suspected July 7th bomber, on CCTV (IPCC, 2007). For Rigoberto Alpizar it may explain in part why he was gunned down at Miami airport.

The power of CCTV 'voice-overs' in identity management is of course demonstrated in the US case of Rodney King in the context of CCTV manipulation and misuse considered above. The extent and the dangers of police voice-overs of CCTV evidence in the UK were highlighted in June 2005. During a criminal case defence lawyers discovered the unqualified status and unreliability of an expert in lip reading who had regularly been employed by the police. The 'expert' has been used to analyse silent CCTV footage in over 700 prosecutions (many of which resulted in convictions). At the time of the discovery the Crown Prosecution Service (CPS) announced that in future where lip reading of CCTV footage is admitted in evidence judges would warn of its limitations and of the risk of error. Nonetheless three subsequent appeals against conviction secured on

the evidence of the discredited 'expert' have failed. Despite defence argument based on the CPS guidelines judges are determined to give weight to the reliability of lip reading evidence of CCTV images. In R v Lutterel[8] the court opined,

> lip reading from a video like facial mapping, is in our view a species of real evidence…We are entirely satisfied that lip reading evidence as to the contents of a videoed conversation is capable of passing the ordinary test of relevance and reliability and therefore being potentially admissible in evidence.

With respect the wisdom of the finding is questionable. The Association of Teachers of Lip Reading for Adults has recommended members do not carry out forensic lip reading for the police since reliability cannot be guaranteed. Professor Quentin Summerfield an expert in linguistics tested the discredited expert's deciphering skills with CCTV footage before her employ by the police. In one test from 297 words she cited 43 that were unuttered and in another 87 (Johnson, 2005). Johnson quotes Jane Hickman of the Criminal Appeal Lawyers Association,

> No one asks, 'How far should we go with forensic evidence?' And its increasingly becoming the whole story in a trial. The trend as science advances is for the Crown to adduce evidence that is not sufficiently developed. Juries are being asked to draw conclusions that the evidence can't bear.

CCTV and the Phenetic Fix

Adey (2004: 502) and Lyon (2002b) talk about the 'phenetic fix' achieved by surveillance technologies that capture in a snapshot the [apparent] essence of movements, bodies and identities[9] [10]. Information obtained from the snapshot is used to determine who might be a threat and should therefore be subjected to more intense security analysis. Before the shooting of De Menezes a grainy CCTV image of a suspected London bomber Hussein Osman was used by the police to determine that De Menezes merited 'another look' (IPCC, 2007: 12.9). This loose determination triggered a train of events that culminated in officers shooting their suspect dead, allegations of police criminality and ultimately to

[8] EWCA Crim 1344, CA (Criminal Division), 28th May, 2004.

[9] Phenetic has the literal meaning of a classification based upon overall similarities.

[10] Walby (2003) conceptualises CCTV as an 'initiating text' which is 'active, activated and contributing to the organisation of sociality and work processes within a ruling framework'. He argues that though prevalent discourses are present in for example the compilation of policemen's' notebooks that the discourse of CCTV permits the *more rapid* reproduction of and circulation of initiating texts in multiple sights as operators participate in and reproduce discourses through meticulous monitoring of citizens. Through these discourses citizens who exhibit certain types of behaviour or characteristics become 'flawed' or 'dangerous', to be dealt with as 'risks to be policed'. Walby notes the pace and immediacy of the labelling of those subject to CCTV surveillance relative to the objects of synoptic media. Conceptualising CCTV as rolling text he found that it *immediately* transformed social relations setting in motion events that *immediately* affected the objects of surveillance.

findings of endangering public safety. Ominously the Stockwell One Report invites the Crown Prosecution Service to consider charges of murder against two officers (IPCC, 2007).

Due process has long been the quarry of a pressurised police force (Williams, 2000; Kaufman, 1998; Anderson and Anderson, 1998). In the wake of the September 11th attacks in America and of the July 7th London bombings due process finds itself closer than ever to becoming the victim of that force. At the forefront of the 'war on terror' it is apparent that CCTV footage increasingly precedes arrest and interrogation as the first point of contact between the police and terrorist suspects. It is arguable that an appearance upon CCTV vies with interrogation, attracting the accolade attributed to the latter by Williams (2000: 209), 'a critical forum in which initial information and impressions are exchanged'. Through the phenomenon of the phenetic fix it may become for the police much more than *prima facie* evidence, as to it they attach a presumption of guilt.

Following the shooting of Rigoberto Alpizar by an air marshal at Miami airport in Florida, statements from fellow passengers indicated that the man had been behaving erratically from an early stage. In fact he was a sufferer of Bi Polar disorder, the symptoms of which include restlessness. Standing in the queue to board he was stated to have been waving his arms about, moving between lines at the Customs check and to have made agitated body movements[11]. There are two distinct types of CCTV, one that records stasis and motion in an environment for the concurrent or subsequent assessment by human and another that records stasis and motion for the concurrent or subsequent assessment by an algorithm (Carroll-Mayer *et al.*, 2006: 3). At many US airports including Miami the 'phenetic fix' is enabled by algorithmic surveillance technologies that analyse CCTV footage in real time. At one level these identify actions such as entering the wrong corridor and on another they pick up on individual body movements. Body movements are 'inscribed with meanings of what is an allowed movement and what is considered suspicious and deviant' (Adey, 2004: 508). Security is alerted to investigate those whose movements are judged by the algorithm to be suspicious or deviant. There is circumstantial evidence to suggest that Mr Alpizar may have been the victim of the 'phenetic fix'. The Marconi Corporation provides Miami Airport with a high speed behavioural recognition surveillance system with integrated access control, video transport, full duplex voice and digital recognition features (Gager, 2005). At the time of installation the system was hailed as a cost saving exercise. It is possible that the price may also be counted in human life. So far the US authorities have refused to acknowledge the involvement of the system in the chain of events leading to the killing of Mr Alpizar. Statements issued by the authorities describe the chain of events as having begun on board when the deceased got up from his seat and ran from the aircraft. If the Marconi system was in operation at the time that Mr Alpizar was passing through Miami airport then it is reasonable to assume that it would have 'noticed' Mr Alpizar much earlier and that security measures against him would have begun from that moment. If this is the case then it is possible that the authorities are attempting to focus attention away

[11] See the final report of Miami-Dad State Attorney's Office http://www.miamisao.com/publications/press/2006/airmarshalshooting.pdf (Last accessed 11th Nov 2007). There are also numerous newspaper reports of witness statements.

from the involvement of CCTV in the debacle[12][13]. Worryingly such an effort would deflect discussion away from the ethical and legal implications of deploying, in the civil setting, autonomous decision systems that identify potential human targets. Ethicists and lawyers pay scant attention to the implications of these devices in the military realm where they are the cause celebre of western military planners (Carroll-Mayer and Stahl, 2005). As they encroach upon the civil setting that apathy becomes more dangerous than ever.

CCTV and the Technological Imperative

In *Speed and Politics* Virilio (1986: 6) proposes 'dromomatics', the influence of speed upon all aspects of urban life, for example transportation, communication and warfare. As computers accelerate and set the pace of human transactions, humans in turn are enthralled to what Virilio terms 'the technological imperative'. There is evidence to suggest that the police and others closely involved with CCTV are subject to the technological imperative; the trite saying 'because the machine says so' takes on sinister meaning as we become what the machine says we are. Manning (1988: 155) posits that technology enslaves officers, '…although the public pays them, they work for the machines that lurk behind them, glow in front of them, click and buzz in their ears and fill the air with electronic sounds'.

This type of response exemplified by, for example, a tendency to respond more to technological 'chat' than to human command in the control based situation, that is well documented (Cummings, 2004: 6). Worryingly it is only very recently, for the first time, and entirely by accident, that the influence of the technological imperative has been noted in the targeting situation. The unexpected results arose from tests undertaken by the US Navy to measure the situational awareness of human controllers of Tomahawk missiles (Cummings, 2004: 5). The tardiness of this discovery was unmodified by situational awareness being as Klein (2000) states 'of utmost importance' to military planners or by previous research by (Ruff *at al.*, 2002) indicating reduced situational awareness arising from poorly designed human/computer interfaces. It is not suggested that the complexity of the military systems is on par with systems such as might be provided by Marconi at Miami airport. It is suggested that human responses to the embedded instant messaging interface in systems such as that provided by Marconi have the propensity to embody the shortcomings identified in the Tomahawk research. Accordingly the potential for catastrophic consequences in air and rail termini and in other surveillance intense environments exists.

---

[12] Discussion of the Marconi system is clouded by obfuscation. Gager (2005) reports Jack Waskowicz head of the program at Miami airport saying of the system that its details 'cannot be revealed'. It is interesting to note also that the system does not appear to have a name though it is however part of the Marconi Simple Multiservice Architecture for Reliable Transport (SMART) programme. Probably the most informative document is one released by Marconi in 2003. Described by the company as a White Paper on Security and Surveillance it was entitled 'Mission Critical Security Network for Critical Infrastructure Protection'

[13] *Editor's Note:* Marconi was largely absorbed by Ericson late in 2005 (Goring, 2005) and most of their reports and documentation are no longer available online or have been rebadged.

Cummings (2004) explains that situational awareness is defined on three levels, 1.Perception of elements in the environment, 2. Comprehension of the current situation, 3. The projection of future status. In the Tomahawk tests controllers were sent routine queries from supervisors in conditions designed to emulate high and low work load periods. Initial analyses revealed nothing out of the ordinary-there were no significant differences in situational awareness despite varying workload levels. However,

> …an unexpected behavioural trend was noted in regards to the use of the instant message interface…Many subjects fixated on the instant messaging and ignored primary tasking of retargeting missiles in urgent situations. This occurred despite the fact that all subjects were repeatedly instructed that retargeting instructions were their primary priority tasking and that answering queries through the chat box was the least important of all tasks…Many subjects would answer all queries before attending to the more pressing retargeting problems…This could be costly from an operational perspective…
>
> (Cummings, 2004: 6).

The chatter from the 'chat box' overrode other more vital tasking information. Cummings emphasises that though these findings were unexpected and did not result from experiments directed at eliciting such information they highlight the need for more research into the effects of instant messaging upon task performance. Manufacturer's literature about digital surveillance systems typically state that the systems analyse,

> images from video surveillance feeds and alert security personnel to behaviours that are suspicious or out of the ordinary, such as a fallen person, lingering individuals or vehicles… predefined behaviours…[14]

The alerts disseminated by systems such as those provided by Marconi equate with 'chat'. It is not known whether the Marconi system did issue 'alerts' at Miami Airport in the incident in question, but if the Marconi system did issue alerts in response to its observation of Mr Alpizar these may have been blindly reacted to by the human agents to the exclusion of other equally valid and important information.

There is evidence tending to suggest that this may have happened. Much has been reported in the press and in the report of Miami-Dade State Attorney's office about Mrs Alpizar having told just about anyone within earshot that her husband's behaviour was being driven by illness. Strangely however this vital information did not impinge upon that collated by Airport security. The unfruitful efforts of Mrs Alpizar are eerily reminiscent of those of the human agents on the ground in Kosovo just prior to the bombing of the Chinese Embassy. On that occasion the systems used to guide bombers mistakenly identified the Chinese Embassy in Belgrade as a legitimate target. Human agents, on the ground, aware of the mistake frantically attempted to intercept the Secure Internet Protocol Router Network (SIPERNET). They failed because SIPERNET is a closed system, incapable of being infiltrated by outside information (Ignatieff, 2000: 64).

---

[14] *Editor's Note*: Cerenium Intelligent Video Analytics site used to be at http://www.cerenium.com However the company no longer exists.

In light of the findings cited by Cummings it is debateable, had it not been a closed system, whether the human voices would in fact have resulted in a countermand to the strike order.

There is another indication that those in charge of the surveillance systems at Miami are, probably unconsciously, acquiescing to the technological imperative. This lies in the unequivocal response of officials when questioned as to how killings like that of Mr Alpizar could be avoided in the future (Cohen, 2005). The officials advocate,

1. Enhanced computer profiling to include more personal information.
2. Increased use of behaviour pattern recognition systems.
3. More explosives detection equipment.
4. People like Mrs Alpizar 'could take on more responsibility to alert the airline of the potential for erratic behaviour that could be mistaken for a threat'.

Now points 1-3 are disquietingly self explanatory. Point 4 however is disturbingly curious. Every day thousands of travellers for myriad reasons are fidgety, irritable or downright obstreperous, they may rush and they may struggle. Many of us, for example, know someone whose fear of flying is physically manifested. The possibilities are infinite. Security experts are effectively saying that as long as humans have the propensity for physical behaviour that is not recognised by algorithms as 'normal' they face execution. Further, execution might be considered legitimate if friends and relatives, having predicted the behaviour in advance or having noticed it, fail to communicate their knowledge to precisely the right people[15].

In 2003 in anticipation of upgrading their surveillance systems in place at US airports, including Miami, Marconi issued a 'White Paper'[16]. The paper described the enhanced capability of the new SMART system,

> In legacy systems integration is achieved via a combination of manual integration and workflow processes. With Marconi SMART solutions the data from all these systems can be fully integrated on the network and monitored via a rule –based approach. The Marconi architecture can take data and events from any and all systems the security manager wants to activate *and the systems can designate the rules that govern how the systems operators react* (italics added).

This approach ignores the cognitive nature of computers. Unlike humans who grow into the position of being moral agents by socialisation, enculturation and learning (Stahl: 2004: 70) computers have no social history from which to form a sense of meaning. Algorithms cannot decide which data is relevant to the construction of morally informed action (Carroll-Mayer and Stahl, 2005: 6).

---

[15] If otherwise suspicious behaviour is to be discounted on the basis of such reports, and they became common, it is hard to see what would stop potential terrorists similarly phoning to advise that their fear of flying may mean that they behave erratically before the flight as a way of deflecting suspicion.

[16] See Note 14.

It is with dismay one notes the complete absence of references to CCTV in the 41 page report issued by the Miami Dade State Attorney's Office exonerating two Air Marshals from guilt in the Alpizar killing. There are hundreds of smart CCTV cameras at Miami Airport yet images from none were referred to in the evidential process. Several still photographs were included in the report but were taken and provided by Miami-Dade police department after the events. The remark made by Gerrard *et al.* (2007: 28) as to state agencies' refusal to discuss publicly their CCTV 'needs' is recalled and takes on refreshed significance in the light of that report. The last paragraph on the last page states:

> It is factually and legally irrelevant whether FAMs 1 and 2 complied with their department's policies and procedures. Whether the Air Marshals' actions are justified or not in the State of Florida is independent of whether they abided by the rules set by a Federal Agency. For this reason, the department's policies and procedures, if any, were not evaluated.

In the face of such obfuscation it is unlikely we will ever know the extent of the involvement of a CCTV system in the death of Rigoberto Alpizar.

The Future and CCTV

If suspects are 'transcarcerated' wider society is transfixed, awaiting mobilization and valorization (Arrigo *et al.*: 2005) from the only voice in the scene, that of the authorities. Hence society waited, believed, and acquiesced as it was told of the execution at Stockwell Tube station of a July 21st 'terrorist' who had been clearly 'identified' from CCTV footage (Cusick, 2005). But now we know the true identity of the man killed as a result of his 'look alike' Hussein Osman having appeared on CCTV; the reliability and the effect of that form of evidence is more roundly understood.

As Dick (2004: 52) reminds, policing is socially constructed. Why then, despite the Menezes and Alpizar killings, evidence suggesting that the police interfere with CCTV evidence, and authoritative findings that CCTV does not reduce crime or increase detection, does the public demand more? In part this is explained by a *sense* of comfort gained from CCTV, the *feeling* that an area is safer. Post September 11th and July 7th Lacan's voice of 'desire' is siren. In the 'war on terror' the social capital of the voice 'on' the CCTV video tape is maximised; offering security, it delivers danger.

At a meeting of the International Association of Public Transport, the then UK Transport Secretary Alistair Darling spoke enthusiastically about the installation of behaviour recognition systems at UK airports and train stations. This was in stark contrast to the opinions of other transport chiefs. Alain Claire, director of the Paris region transport authority, rejected Darling's objective. Claire cites the greater accuracy of human security agents. Attention was drawn to recent unsuccessful trials of behaviour recognition technology in one London station. Results indicate the vast majority of alerts triggered by the system were mistakes (Mathews, 2005). Just such a 'mistake' may have led to the death of Alpizar. Consensus among conference delegates is that the systems are immature and unreliable. This has not however dampened the zeal of the authorities.

Speaking contemporaneously Ian Johnston, Head of British Transport Police, was adamant that the systems are needed now (Davenport, 2005). Marconi continued to have involvement with security systems at a European level including the Paris Metro, Eurotunnel and London Underground (Gerbig, 2003). In 2005 Marconi Transportation was awarded a £150 million contract to install and operate surveillance on three London Underground lines; Northern, Piccadilly and Jubilee (Datamonitor, 2005)[17]. If the UK surveillance policy continues upon its current trajectory it is likely that society will become increasingly dominated and eventually framed within what might be termed the 'double glazing' of advanced surveillance technology. CCTV images of human beings as they traverse the boundaries of social order, through the centres of mobility will be routinely processed, characterised and sorted, by algorithm into one of two categories- potential or confirmed targets of lethal force.

Conclusion

This paper is a critical analysis of the implications of CCTV identity management technologies for the criminal justice process. The consideration was undertaken in response to the call by the UK Presidency of the EU to expand the deployment of CCTV surveillance technologies. The paper counter poses and supplements assumptions pertaining to CCTV technologies that emanate from the policy making cadre; it looks beyond the standard utilitarian stance. Fear of the manipulation and misuse of CCTV technologies in the criminal justice process has haunted the technology since its inception as an instrument of the law. In the section devoted to this issue the paper examined opportunities for manipulation and misuse and demonstrated the realisation of the fears as they manifested in the remarkable case of Rodney King. The paper examines concepts that loom on the postmodernist agenda; transcarceration, the phenetic fix and the technological imperative and through their lens exposed the characteristics of CCTV technology to critical analysis.

The paper looked at the effects of CCTV surveillance *in extremis* as they intermingled to a greater or lesser extent with the other causal factors affecting the deaths of Rigoberto Alpizar and Jean Charles De Menezes in the CCTV rich environments of airports and train stations. It considered the nature of these environments, reconstructed through technologies of surveillance by 'the new experts in the situational', as they displace experts whose remit was the individual and the social. Casting the reconstructed CCTV rich environments of the airport and the station as prescient microcosms of other/wider spaces the paper illuminated the societal pitfalls. In sum the paper draws attention to research findings tending to suggest that inadequately considered reliance upon CCTV evidence promises the worst of all possible worlds, a world where crime is not in fact reduced, where the legitimate forces of law may themselves be compromised and the identity of the individual ultimately lost. It is time to interrogate the strengths and weaknesses of CCTV technology, its power to mislead and openness to abuse so that its capabilities can be better harnessed to draw in tandem the interests of the criminal justice system and of the individuals affected by it.

[17] See Note 14.

References

Adey, P. (2004) *Secured and Sorted Mobilities: Examples from the Airport*, Surveillance and Society 1 (4): 500-519. http://www.surveillance-and-society.org/articles1(4)/sorted.pdf

Anderson, B and D. Anderson (1998) *Manufacturing Guilt: Wrongful Convictions in Canada*, Halifax, Fernwood Books.

Arrigo, B.A. (1997a) Transcaraceration: Notes on a Psychoanalytically-informed Theory of Social Practice in the Criminal Justice and Mental Health Systems, *Crime Law and Social Change: An International Journal* 27(1): 31-48.

Arrigo, B.A. (2001b) Transcaration: A Constitutive Ethnography of Mentally Ill Offenders, *The Prison Journal* 81(2):162-186.

Arrigo, BA., D. Milovanovic and R.C. Schehr (2005) *The French Connection in Criminology: Rediscovering Crime Law and Social Change*. Albany New York: SUNY Press.

Bondarauk,. T. and R. Hubb (2003) *Discourse Analysis: Making Complex Methodology Simple*. Cambridge: Polity Press.

CameraWatch Launch Report, May 30th, 2007 http://www.camaerawatch.org.uk/press/june07/CameraWatch_post_launch_release_final.pdf (Last accessed October 4th, 2007).

Carroll-Mayer, M. and B.C. Stahl (2005) The Wild West: Nanotechnological Weaponry and the Rule of Law on the Battlefield, British and Irish Law Education and Technology Association, 20th BILETA Annual Conference. Queens University, Belfast, 6th-7th April, 2005.

Carroll-Mayer, M, Fairweather. B, and Stahl B (2006) Ignotious Per Ignotum: 21st Century Surveillance Technology and the Presumption of Guilt, *British and Irish Law Education and Technology Association, 21st BILETA Annual Conference.* Malta, April 2006.

Datamonitor (2005) *Marconi wins £150 million London Underground Contract*, 26th Jan 2005 http://www.datamonitor.com/industries/news/article/?pid=F11014B5-69AD-43C4-B860-A5FDC406DEC8&type=NewsWire (Last accessed 18th Jan 2008)

Chong, P., S. Ho and B. Arrigo (2006) Reality Based Television and Police Citizen Encounters, *Punishment and Society* 8(1): 59-85.

Coffey, M. and Hannigan B (2005) Community mental health in the UK: restructuring for the 21st century, *Sociale Psychiatrie* 24(75): 25-30

Cohen, M. (2005) 'Experts stand behind air marshal in Miami incident', Baltimore Sun Dec 9th. http://archive.southcoasttoday.com/daily/12-05/12-09-05/a07wn633.htm (last accessed Jan 18th 2008)

Cusick, J. (2006) An Innocent Man Shot Dead on the Tube by Police. *Sunday Herald* Aug 21st http://findarticles.com/p/articles/mi_qn4156/is_20050821/ai_n14915960 (Last accessed Jan 18th 2008)

Crang, M. (2002) Between Places Producing Hubs Flows and Networks-Introduction. *Environment and Planning*, A 34(4): 569-574.

Cummings, M.L. (2004) The Need for Command and Control Instant Message Adaptive Interfaces: Lessons Learned from Tactical Tomahawk Human in the Loop Simulations, *Cyber Psychology and*

Behaviour, 7(6): 653-661

Cunningham, I. (2007) *CameraWatch Launch Report*, May 30th, 2007 http://www.camaerawatch.org.uk/press/june07/CameraWatch_post_launch_release_final.pdf (Last accessed October 4th, 2007).

Cusick, J. (2005) An Innocent Man Shot Dead on the London Tube by Police, Sunday Herald, 21st August http://findarticles.com/p/articles/mi_qn4156/is_20050821/ai_n14915960 (Last accessed 18th Jan 2008)

Cwerner, S. (2006) conference web page *Air Time-Spaces: New Methods for Researching Mobilities*, Lancaster University, UK, 29TH-30 September 2006 http://www.lancs.ac.uk/fass/sociology/cremore/airspaces/airspaces.htm (Last accessed November 3rd, 2007).

Davenport, J. (2005) London Tubes To Use High Tech Explosives Scanners, *Evening Standard*, November 15th, 2005.

Dick, P. (2004) The Position of Policewomen: A Discourse Analysis Study. *Work Employment and Society*, BSA publications, 18:1, Sage Publications: Thousand Oaks: New Delhi.

Edwards S.M. (2002) *Perjury and Perverting the Course of Justice Considered* available at http://74.6.146/search/cache?ei=UTF-8&p=perverting+course+of+justice+uk+police&rd=r1&u=www.buckingham.ac.uk/publicity/articles/edwards-paptcojc.pdf&w=perverting.pdf. Last accessed October 7th, 2007.

Fay, B. (1987) *Critical Social Science: Liberation and Its Limits*, Polity Press Cambridge.

Ferrie, G. (2007) *CameraWatch Launch Report*, May 30th, 2007 http://www.camaerawatch.org.uk/press/june07/CameraWatch_post_launch_release_final.pdf (Last accessed October 4th, 2007)

Foundation for Information Policy Research (FIPR) (2003) *Surveillance and Security*, http://www.fipr.org/surveillance.org (Last accessed Nov 11th 2007).

Foucault, M. (1977) *Discipline and Punish: The Birth of A Prison*. New York: Pantheon.

Freud, S. (1914) *The History of the Psychoanalytic Movement*, translated by A.A. Brill http://psychclassics.yorku.ca/Freud/History/index.htm

Gager, R. (2005) Multiplying Surveillance Eyes http://www.objectvideo.com/objects/pdf/articles/2005_01_SDM.pdf (Last accessed Jan 18th 2008).

Gerbig P. (2003) Network Based Prevention: Multiservice-Networks for Security http://www.euro-police.com/pdf/gerbig.pdf (Last accessed Nov 9th 2007)

Gerrard G., G. Parkins, I. Cunningham, W. Hill, S. Jones and S. Douglass (2007) *The National CCTV Strategy*, Report for the Home Office, October 2007 http://www.crimereduction.homeoffice.gov.uk/cctv/cctv048.pdf (Last accessed Nov 11th, 2007)

Gill, M. and A. Spriggs (2005) Assessing the Impact of CCTV. *Home Office Research Study* 292 Feb 2005, http://www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf (Last accessed Jan 18th 2008).

Goodwin, C. (1994) Professional Vision, *American Anthropologist* (New Series) 96(3): 606-633. http://sscnet.ucla.edu/clic/cgoodwin/94prof_vis (Last accessed Nov 2nd 2007)

Goold, B. J. (2003) Public Area Surveillance and Police Work: The Impact of CCTV on Police Behaviour and Autonomy, *Surveillance & Society* 1(2):191-203

Goring, N. (2005) Ericsson to buy most of Marconi for $2.1B: Ericsson acquires Marconi's optical networking equipment, broadband access and softswitch products. *IDG News Service*, October 25. http://www.infoworld.com/article/05/10/25/HNericssonmarconi_1.html (Last accessed Jan 18th 2008).

Haggerty K.D. (2004) Displaced Expertise: Three Constraints on the Policy-Relevance of Criminological Thought, *Theoretical Criminology* 8(2): 211-231

Hickman, J. (2005) quoted in *Downfall of the Silent Witness*, interview with Angela Johnson, Mail on Sunday, July 10th 2005.

Home Office (2007) *Talking CCTV brings voice of authority to streets*, 4th April 2007 http://www.homeoffice.gov.uk/about-us/news/talking-cctv (Last accessed Nov 2nd, 2007).

House of Lords Science and Technology Select Committee, Fifth Report, *Digital Images as Evidence*, 3rd February 1998.

Ignatieff, M. (2000) *Virtual War: Kosovo and Beyond*, London: Metropolitan Books.

Introna, L. and D. Wood (2004) Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems, *Surveillance & Society* 1(2): 177-198.

Independent Police Complaints Commission (IPCC) (2007) *Stockwell One: Investigation into the Shooting of Jean Charles Menezes at Stockwell Underground Station*. London: IPCC. http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_11_07_stockwell1.pdf (Last accessed 18th Jan 2008)

Johnson, A. (2005) Downfall of the Silent Witness, *Mail on Sunday*, July 10th 2005.

Kaufman, F. (1998) *Commission on proceedings involving Guy Paul Morin*, Toronto: Queen's Printer For Ontario. http://www.attorneygeneral.jus.gov.on.ca/morin/morin.htm (Last accessed Jan 18th 2008)

Klein, G. (2000) Analysis of Situational Awareness from Critical Incidence Reports. In D.J. Garland (ed.), *Situation Awareness Analysis and Measurement*, 51-71, Mahwah: New Jersey: Lawrence Erlbaum Associates.

Lacan, J. (1977) *Ecrits: A Selection*. Trans A. Sheridan. New York: W.W. Norton.

Lowman J., R. Menzies and . Palys (eds.) (1987) *Transcarceration: Essays in the Sociology of Social Control*, Aldershot and Gower.

Lyon, D. (2003) Airports as Data Filters: Converging Surveillance Systems after September 11th.*Information, Communication and Ethics in Society*, 1(1):13-20.

McCahill M. and C. Norris (2002) *CCTV in London*, Working Paper No 6 http://www.urbaneye.net/results/ue_wp6.pdf (Last accessed Jan 18th 2008)

Manning, P. K. (1988) *Symbolic Communication: Signifying Calls and the Police Response*. Cambridge Massachusetts: MIT.

Mathews, J. (2005) *Hi tech, High Transport Security?* BBC News, 14th November 2005 http://news.bbc.co.uk/1/hi/uk/4435998.stm (Last accessed Jan 18th 2008).

Murakami Wood, D. (ed.), K. Ball, D. Lyon, C. Norris and C. Raab (2006) *A Report on the Surveillance*

Society, Wilmslow, UK: Office of the Information Commissioner / Surveillance Studies Network. http://www.ico.gov/upload/documents/library/data_protection/practical_application/surveillance_society_public_discussion_document-06.pdf (Last accessed November 1st, 2007)

Norris, C. and R. Armstrong (1999) *The Maximum Surveillance Society: The Rise of CCTV*. Oxford: Berg.

Phillips, P.P. *et al.* (2003) *Face Recognition Vendor Text 2002, Overview and Summary* http://biometricinstitute.org/bi/faceRecognitionVendor Test2002.pdf (Last accessed Nov 2nd, 2007)

Potter, J. (1996) Discourse Analysis and Constructionist Approaches: Theoretical Background, in J.T.E Richardson (ed.) (1996) *Handbook of Qualitative Research Methods for Psychology and the Social Sciences*, 125-140, Leicester: BPS Books.

Riley, T.B (2004) *Security and Privacy: Striking the Right Balance*, Centre for Electronic Governance http://www.electronicgov.net/pubs.research_papers/slp/Sec&PrivPaper03y03pdf (Last accessed Nov 11th, 2007)

Ruff, H., S. Narayanan and M. Draper (2002) Human Interaction With Levels of Automation and Decision Aid Fidelity in the Supervisory Control of Multiple Simulated Unmanned Aerial Vehicles, *Presence II* (4):325-351.

Semple, J. (1987) Bentham's Haunted House. *The Bentham Newsletter*, 11:35-44.

Stahl, B. C. (2004) The Ethics of Critical IS Research, *Proceedings of the 2nd International Conference on Critical Research in IS Workshop*, 14th July, 2004.

Virilio, P. (1986) *Speed and Politics*, New York, Semiotext(e).

Walby, K. (2003) How Closed-Circuit Television Surveillance Organises the Social: An Institutional Ethnography, *Canadian Journal of Sociology* 30: 189-214.

Werrett, S. (2003) Potemkin and the Panopticon: Samuel Bentham and the Architecture of Absolutism in Eighteenth Century Russia, *Journal of Bentham Studies*, 2. http://eprints.ucl.ac.uk/648/

Williams, J. W. (2000) Interpreting Justice: A Critical Analysis of Police Interrogation and Its Role in the Criminal Justice Process. *Canadian Journal of Criminology* 42: 209-241.

Cases

R v Archer 2002, (unreported) Smith Bernel, Case No. 0104555 S2.

R v Lutterall 2004, EWCA Crim 1344, CA (Criminal Division), 28th May.