BILETA 21st BILETA Conference: Globalisation and Harmonisation in Technology Law
British & Irish Law, Education and Technology Association April 2006, Malta.

Ignotious Per Ignotum: 21st Century Surveillance Technology and the Presumption of Guilt.

Moira Carroll-Mayer, N Ben Fairweather, Bernd Carsten Stahl.
The Faculty of Computing Sciences and Engineering, De Montfort University
moiracaroll2000@yahoo.co.uk : nbf@dmu.ac.uk : bstahl@dmu.ac.uk,

Abstract

The UK Presidency of the European Union is calling for an expansive, mandatory policy of surveillance aimed at the reduction of crime.

There is evidence to suggest that the proposed policy, to be implemented through the medium of second generation surveillance technology, will lead to the effective deregulation of the police and security forces and impliedly to erosion of the rule of law. As second generation surveillance technology increasingly replaces arrest and interrogation as the first point of contact between the police and the suspect it is time to interrogate whether the Panoptic ideal is being undermined.

This paper accordingly goes beyond the Foucauldian chain of equivalence between visibility, vulnerability and subjectification to assess whether surveillance can be equated with discipline in the 21st century. The assessment based upon a critical analysis of reported interactions between the police, security forces and suspects in surveillance intense environments concludes that exposure to the stimuli of second generation surveillance technology may produce effects that are the antithesis of those anticipated by the Panopticism. The paper answers calls being made to address the implications of second generation surveillance technology for the rule of law.

1. Introduction

On the 7th September 2005 the European Presidency released its first formal report on security enhancement entitled Liberty and Security: Striking the Right Balance[1]. The title of the report suggests that the proposed initiative is reconcilable with a rule of law underwritten by humanitarian influences. The report proffers the transmutation into European law of failed UK voluntary surveillance policies underscored by a modus operandi that is dictated by algorithmically enhanced CCTV surveillance technology. The rationale is that expansive surveillance will promote the prevention, investigation and prosecution of 'ordinary' crimes and terrorism. These aspirations do not reflect the findings of a study undertaken for the Home Office by Gill and Spriggs (2005:120) that CCTV does not have a favourable impact upon crime. Facts are losing out however in the post 9/11 surveillance surge as those with an interest in surveillance technologies promote them to a traumatised polity (Introna and Wood: 2004:1). We should look to see if the rule of law in tandem with common sense is heading towards negation so that remedial action can be taken.

The call of the Presidency testifies to the perennial allure of the Panopticon. That it fails to reduce crime and in cases perpetuates and engenders that which it is designed to eradicate should not surprise if it is understood that the Panopticon was designed to control the unauthorised activities of overseers. Hijacked for purposes of societal control the Panopticon in all its forms draws us again and again back to the question of 'who shall guard the guards?' (Carroll-Mayer and Stahl: 2006:1).

There is near consensus that the presence of CCTV in the working environment of police officers engenders negative and criminal behaviour on their part (Werrett: 2003:192). Norris and Armstrong (1999:190) cite officers signalling operators to pan away from their questionable activities. The tendency to ignore and suppress footage, attempts to remove tapes recording police misconduct, officers coming to control rooms to 'check the evidence', officers failure to see themselves bound by the Codes of Practice on CCTV evidence handling and access are recorded by Goold (2003).

[1] The report may be accessed at http://www.privacyinternational.org/issues/terrorism/library/ukpresidencypaperonstrikingtherightbalance.pdf

According to Gould officers view CCTV evidence as existing primarily for their benefit and regard themselves as the rightful owners of CCTV evidence.

So what's new? Everything is not as it should be regarding officers' behaviour. But there are more insidious, consequently more dangerous forces at work in the CCTV environment to undermine the rule of law, that threat matched only by the ironic determination of the law to look the other way. There are two distinct types of CCTV, one that records stasis and motion in an environment for the concurrent or subsequent assessment by a human and another that records stasis and motion in an environment for the concurrent or subsequent assessment by an algorithm. It is the latter, commonly referred to as 'smart' CCTV, which presents the greatest threat to the rule of law.

There has been a good deal of commentary concerning the evidential value and the consequences of suspect identification by humans from CCTV footage. Bromby (2002, 2005) describes how e.g. the prevalence of shadow, motion blur, changes in facial expression and faces turned at more than 45% away from the camera can reduce the probative value of CCTV evidence. Where images are of a very poor quality they are carefully examined by an expert in facial mapping. The expert prepares a report that addresses and explains the effects that are detrimental to the image and s/he indicates how these make it more or less likely that the CCTV image is that of the suspect or defendant. This type of painstaking scenario in the police station and in the court room is not replicated in the everyday CCTV environment of airports and train stations where CCTV footage is collected in situations of heightened security awareness and evaluated not by a human being but by an algorithm in the temporal immediacy of real time. In this type of CCTV environment the evidence of the suspect's guilt is unlikely to be either evaluated or acted upon in accordance with what we over centuries have come to recognise as the due legal process.

It is notoriously difficult to log and interrogate the evidence trail produced by algorithmically enhanced CCTV, it becomes impossible to inspect or to trace the codes operation as they are involved in multiple layers of translations for execution, to trace the connection between currents flowing through silicon chips as they translate

into programme instructions and to tell if the code being examined is the code that was actually executed at the time of the action pertinent to the legal investigation.

Though it is possible to go through the code line by line it is not possible to see it in operation. As Introna and Wood (2004:183) put it because of this 'CCTV software algorithms are operationally obscure'. The difficulties are compounded by there being a mere handful of experts worldwide with the ability to understand and interpret the algorithmic trail left by smart CCTV, even they confused by the obscurity of the CCTV evidence trail (Philips et al 2003).

In 1998 the House of Lords Select Committee on Science and Technology drew attention to the possibilities digital CCTV presents for unacceptable manipulation as averse to acceptable enhancement of images used for evidential purposes and to the difficulties of establishing an acceptable audit trail. The Committee concluded that observers should have no more faith in what they saw on CCTV than on paper text presentations of questionable provenance. On the question of the audit trail the Commission said 'no defence team in the UK had as yet ever requested an audit trail in cases where video images were being used'. The Committee attributed this to lack of familiarity with digital technology. The issue of audit trails of digital evidence has been attended to since 1998. It cannot be supposed that in 1998 the Commission anticipated algorithmically enhanced CCTV technology capable of evaluating behaviour and of summoning lethal intervention. The extent of the involvement of 'smart' CCTV in incidents such as the Stockwell tube station and Miami airport shootings should not go unaddressed due to the operational obscurity of that technology.

2. Inherent Bias in Smart CCTV Systems

Operational obscurity is exacerbated in the case of proprietary smart CCTV systems as commercial enterprises seek to protect their interests and where it is typically claimed of systems that they are unbiased in relation to skin colour, race and gender differences. The claim is made by for example by Lake Systems, reportedly the providers of Cromatica CCTV to London Underground[2] for use on the Northern Line.

[2] www.lakeimage.com also www.ats-computers.com/biometrics/face.html

This line incorporates Stockwell tube station the lighting of which is considered by Lake Systems to be especially conducive to the employ of CCTV[3].

Introna and Wood (2004:2) allege that the algorithms in CCTV systems do not treat all faces equally; they cite the question posed by Agre (2003) 'what happens if faces are used by CCTV systems as bar codes?' The idea that faces could be used as bar codes by CCTV technology is more than hypothesis. How can this be? A CCTV system requires a database of faces against which it compares the faces of those it 'sees'. It does this by creating a template of the passing face. The faces on the database vary with the operational context of the system e.g. at a library it could contain the faces of members, at an airport it could contain the faces of terrorist suspects. If there is a match an alarm is issued to human security operatives so that they will take 'appropriate' action. Generally the higher the state of alert the greater will be the number of false alarms[4]. It is widely disseminated by marketing organisations and by organisations employing smart CCTV systems that human operatives will assess and address false alarms appropriately. This claim is questionable in light of research by Cummings (2005) and will be discussed below.

The CCTV systems in operation at airports and increasingly at rail stations contain one of two types of algorithms; Image Template and Geometry Feature Based.

Image Template algorithms compare the face of the passer by with a gallery of face images to single out distinctive features. This is an intuitive approach somewhat reminiscent of human recognition techniques and bias is in built.

Geometry Feature Based Algorithms conduct what is called Local Face Analysis. The algorithms locate points at the eyes, nose, and mouth and connect the points to form a net on which are imprinted the distances between these features. A problem is that this system is relatively less sensitive to lighting, skin tones, eye colour, shape, glasses, hair style and pose than that of the Image Template. Tests show that the system does not have an inbuilt bias but that it can develop one e.g. towards those of a particular ethnic group the features of which deviate from those of the majority.

[3] Ibid
[4] See an article released by AC Controls @www.accontrols.co.uk

Tests conducted in 2002 by the Defence Advanced Research Projects Agency, the Department of State and the FBI using a database of 37437 people of Mexican origin revealed definite bias. Males were recognised accurately 6-9% more often than females while overall figures for both genders were 78% accurate for males and 79% for females. Different age groups attracted widely varying degrees of accuracy; for 18-22 year olds accuracy was a mere 62%, 38-42 year olds attracted 74% accuracy and between 42 and 63 accuracy reduced by 5% every 10 years (Introna and Wood 2004:189). Separate research conducted by Givens et al (2003) into smart CCTV bias clearly identified a significant race bias, Asians and Afro-Americans are more easily recognised than whites, while other races are in general more easily identified than whites. Older people of all races and colours are more easily identified.

Introna and Wood (2004:190) highlight other problems revealed in tests conducted by the Tampa Police Authority, the FBI and Miami Airport Authority that endanger innocent individuals. An image of an unknown person was compared by the system to check for accuracy of identification.

Results were disturbing; for every year between the original entry to the database and comparison of the unknown face reliability reduced by 5%. Each time the database doubled its size its accuracy was reduced by between 2-3%. Pertinently Introna and Wood cite the experiences in 2002 of the Tampa Police Department and of Miami airport officials with smart CCTV systems. In Tampa the CCTV system was abandoned due to all the false alarms while at Miami airport the false alarm rate was 53% (we do not know if Miami airport abandoned that system or if it is the system in operation -thought to be Sentryexit). In the UK at Newham a system called FaceIt failed to make a single correct identification.

The reported tension between CCTV controllers and the police reported by Goold (2003) is redolent of that which allegedly arose between rail officials and the police as to the whereabouts or existence of the CCTV footage pertinent to the killing of Jean Charles De Menezes at Stockwell Tube station in London.

The killing of Jean Paul De Menezes and of Rigoberto Alpizar by members of the police force both within high intensity CCTV environments, a London underground station and an American airport, stand testimony to the need to take a long hard look

at the implications for the rule of law stemming from reliance upon smart CCTV technology. In the Menezes case CCTV cameras are implicated at two crucial stages.

Before the shooting a grainy CCTV image of a suspected London bomber was used to determine that De Menezes merited ‘another look’ by his colleagues. This loose determination triggered a train of events that culminated in officers shooting their suspect dead and to allegations of police criminality. CCTV cameras again became the touchstone for allegations of police criminality when video recordings of the victim and of events leading up to and including his killing disappeared.

When Jean Paul De Menezes was killed at Stockwell it is possible that the ‘Cromatica’ system was operational and when Roberto Alpizar was killed at Miami airport the ‘Sentry Exit’ system may have been. We have heard allegations that the facial recognition software components built into smart CCTV systems, exemplified by ‘Cromatica’ and ‘Sentry Exit’, contain an inherent bias. Is there anything about the killings of De Menezes and Alpizar that substantiates these claims? It is not likely, certainly in the present security environment that the answer to this question will easily be found. However to borrow a phrase, from an arguably not unrelated area of the law, there is a ‘striking similarity’ in the appearance of Osman Hussain the first suspect for the failed July 21st bombings attempts in London captured on smart CCTV, that of Jean Paul De Menenzes shot at Stockwell tube station and of Rigoberto Alpizar shot after that at Miami airport.

Justice and due process have 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 justice and due process threaten to become the victim of that force. At the forefront of the ‘war on terror’ CCTV footage increasingly replaces arrest and interrogation as the first point of contact between the police and suspect. Williams said of interrogation, it becomes ‘a critical forum in which initial information and impressions are exchanged’. The same might be said of the appearance of a suspect upon a CCTV screen, it may become for the police much more than prima facie evidence as to it they attach a presumption of guilt.

Of course appearances upon publicly located CCTV screens are unaccompanied by a voice. They acquire, in the hands of the police however, a ‘voice over’. The absence of a voice is important. The superimposition of the voice of the police 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 criminalisation of those depicted on CCTV. It perhaps partially explains the horrifying results, for Charles De Menezes, of the appearance of his look-alike on CCTV. For Rigoberto Alpizar it may explain in part why he was shot at Miami airport.

Of airports Adey (2004:1477) has this to say ‘they are symbols of mobility, emblematic of the post modern world… well and truly a space under surveillance’. They are however unnoticed by the social sciences, ‘non places’ (Crang: 2002) their role in surveillance, largely ignored, reflects that invisibility and demonstrates an arena wherein the rule of law is directly and unopposedly challenged by surveillance technology. What happens at airports, and surely now at rail stations, is a microcosm of events to come in wider society (Lyon: 2003). We may learn useful lessons from what happens there for other places and spaces. Airports [and rail stations] are centres of mobility, 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 a societal struggle for the right to determine the rule of law.

3. In a Movie Prison

This paper now compares society’s characterisation on TV of those considered mentally ill, the expunging and dubbing of their voices with authorities’ response to ‘suspects’ on CCTV. It concludes that suspects on CCTV are silenced more effectively and judged less favourably than the mentally ill.

The postmodernist critique defines the constitution of society’s punishment of the mentally ill in terms of linguistic and symbolic structuralism (Chong et al 2006). This is exemplified for example by what Arrigo (1997and 2001) calls ‘transcarceration’ the process by which the mentally ill are perceived on television to be routed to and from civil or criminal confinement settings. In this setting the sense making speech is located in the unconsciousness of the viewer ‘awaiting mobilization and valorization’

(Arrigo et al: 2005). Consciousness refers to the level and type of awareness experienced about a person, phenomenon or situation or to a combination of these (Freud 1914 cited by Chong et al p.62). For Lacan (1977) these constituents are the locus of a pivotal divide through which individuals desires are spoken, unspoken, presented, concealed, mobilized or repressed. Desire is the representation therefore of circumscribed, highly subjective knowledge. The intensity, duration and frequency [and effectiveness] of the 'desire' vary with the social capital conferred upon the speaker by those in the listening environment.

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 clinicolegal system of communication. The latter is identifiable in the articulation of self referential, thematic, circulated meanings and values of the clinicolegal professions.

Clinicolegal 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 clinicolegal communication setting the mentally ill are over time homogenised, pathologised and 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 by the police for identification purposes. Not for him a luxurious world where the forces of linguistic and symbolic structuralism triumph over the validity of the mentally ill, where disempowered voices are nonetheless heard from 'the plane of meaning and being' (Chong: 2005). In the silent movie world of CCTV police 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, loiterering 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, a 'manifestation of punishment assuming a discursive linguistic form'.

4. Trapped by 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. Information obtained from the snapshot is used to determine who might be a threat and should therefore be subjected to more intense security analysis. Following the shooting of Rigoberto Alpizar by an air marshal at Miami 27airport 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 disease the symptoms of which include restlessness. Standing in the queue to board he had been waving his arms about and his other body movements indicated he was agitated. At many US airports 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 but 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 evidence to suggest that Mr Alpizar was the victim of the 'phenetic fix'. In 2003 the Cernium Corporation installed Sentryexit behaviour recognition system [5] at Miami airport Florida[6]. At the time the installation was hailed as a cost saving exercise. The price may also be counted in human life. So far the US authorities have refused to acknowledge the involvement of Sentryexit in the chain of events leading to the killing of Mr Alpizar. It was only by checking trade literature that this writer was able to establish the probable presence of Sentryexit at Miami at the time of Mr Alpizar's death. All 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 Sentryexit 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. The authorities appear to be at pains to focus attention away from the involvement of CCTV in the debacle.

[5] Sentryexit is specifically referred to by Adey (2004:5080.

[6] See 'Cerenium installs security system at Palm Beach airport' in The St Louis Business Journal, July 16 2003 @www.bizjournals.com/stlouis/stories/2003/07/14/daily38.html last accessed December 7 2005. The system is used worldwide in prisons, airports etc. See www.cerenium.com/news.

Worryingly their effort distracts from the involvement, in the civil setting, of autonomous decision systems that identify potential human targets. Ethicists pay scant attention to these devices in the military realm where they are the cause celebre of western military planners (Carroll-Mayer and Stahl: 2005). As they encroach the civil setting that apathy becomes more dangerous than ever.

5. All Caught Up in Cyber World

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’. It is entirely possible that the police are subject to the technological imperative. 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 control based situations is well documented (Cummings:2004:6). Worryingly it is only very recently, for the first time and entirely by accident that this effect has been related by developers to the targeting situation. This is despite situational awareness being considered ‘of utmost importance’ (Klein: 2000). Previous research identified reduced situational awareness with poorly designed human/computer interfaces (Ruff, Narayanan and Draper 2002). Cummings (2004:5) reveals the unexpected results of tests undertaken by the US Navy to measure the situational awareness of human controllers of Tomahawk missiles. It is not suggested that the complexity of these systems is on par with those of the human controllers of systems such as Exitsentry. It is suggested that human responses to the embedded instant messaging interface in systems such as Exitsentry have the propensity to replicate those identified by the Tomahawk research with catastrophic consequences for those passing through air and rail termini. Cummings 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 tests controllers were sent routine queries from their 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' invariably 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. Trade literature about Sentryexit states that the system,

> '…analyses images from video surveillance feeds and alerts security personnel to behaviours that are suspicious or out of the ordinary, such as a fallen person, lingering individuals or vehicles…16 predefined behaviours…'

The alerts disseminated by Sentryexit equate with 'chat'. If Sentryexit 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.

Much has been reported 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 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

Kosovo 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, one reason being that SIPERNET is a closed system, incapable of being infiltrated by outside information. In light of the findings cited by Cummings it is debateable whether had it not been closed the human voices would 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[7]. The response advocates,

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. Most for example know someone whose fear of flying is physically manifested. The possibilities are infinite. Security experts are in fact saying that as long as humans have the propensity for physical behaviour that is not recognisable by algorithms as 'normal' they legitimately face execution. 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).

[7] Meredith Cohen 'Experts stand behind air marshal in Miami incident', Baltimore Sun @www.southcoasttoday.com/daily

6. Would You Like Some More?

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 police. Hence society waited, believed and acquiesced as it was told of the execution at Stockwell Tube station of a July 7th ‘terrorist’ who had been clearly ‘identified’ from CCTV footage. But now we know the true identity of the man killed on foot of CCTV evidence, and 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 Menendez and Alpizar killings, evidence suggesting that in relation to those, and routinely, the police interfere with CCTV evidence, accepted 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. Asked ‘Would you like some more security?’ society unlike the wiser Alice, who knew she hadn’t been given any tea yet by the Mad Hatter, replies ‘Yes please’.

At a meeting of the International Association of Public Transport the 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’ probably 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 police. Speaking contemporaneously Ian Johnston Head of British Transport Police was adamant that the systems are needed now (Davenport: 2005). It is likely that a layered model, increased numbers of rail staff on platforms, increased security

personnel and high tech equipment will be introduced in the short term here. If the UK surveillance policy continues upon its current trajectory it is likely that surveillance here, as in the US, will become increasingly dominated by what I term ‘double glazed’ technology, CCTV images of human beings processed, characterised and allocated membership, by algorithm, of one of three categories - non, potential or confirmed targets of lethal force.

7. Conclusion

This paper focused upon the irreconcilability of the plan of the European Presidency to ensure CCTV coverage across states with the rationale of crime prevention and the endurance of the rule of law. In particular it drew attention to research findings tending to suggest that increased reliance upon CCTV evidence promises the worst of all possible worlds, a world where crime is not infact reduced and where the forces of law are themselves compromised to the point of criminality. In order to demonstrate the connection between a possible propensity for the intensification of criminal activity and the presence of CCTV the paper drew upon reports of the killings of Jean Charles De Menenzez and of Rigoberto Alpizar that occurred in CCTV rich environments. The paper presented prima facie evidence of the direct involvement of CCTV technology in those killings. The paper considered in more general terms too the implications for suspects of appearing in CCTV footage. CCTV footage is becoming more and more the ‘ordinary evidence’ of the criminal process. It is time to interrogate its strengths and its weaknesses, its power to mislead and its openness to abuse, lest like the White Rabbit we are heard to cry ‘I’m so late! I’m so very late’.

References

Adey Peter (2004) *Secured and Sorted Mobilities: Examples from the Airport*, Surveillance and Society 1 (4), pp 500-519.

Agre PE (2003) *Your Face is not a Bar Code: Arguments Against Face Recognition in Public Places* @http://dlis.gseis.ucla.edu/pagre

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

Arrigo BA (1997) *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), pp31-48.

Arrigo BA (2001) *Transcaration: A Constitutive Ethnography of Mentally Ill Offenders*, The Prison Journal 81(2), pp162-186.

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

Bromby Michael and Haley Ness (2005) *Over Observed: What is the Quality of this New Digital Legal World?* BILETA Annual Conference,QUB, Belfast April 2005.

Carroll Lewis (1866) *Alice's Adventures in Wonderland*, New York, D Appleton and Company.

Carroll Lewis (1872) *Through the Looking Glass*, London Macmillan.

Carroll-Mayer Moira and Stahl Bernd Carsten (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.

Chong Philip, Ho Shon and Bruce A Arrigo (2006) *Reality Based Television and Police Citizen Encounters*. Punishment and Society, Vol 8, No 1, pp 59-85.

Cohen Meredith (2005) '*Experts stand behind air marshal in Miami incident'*, Baltimore Sun @www.southcoasttoday.com/daily

Crang M (2002) *Between Places Producing Hubs Flows and Networks-Introduction. Environment and Planning* A 34 (4), pp569-574.

Cummings ML (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, 2004, Vol 7 (6).

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

Dick Penny (2004) *The Position of Policewomen: A Discourse Analysis Study*. Work Employment and Society, BSA publications, Vol 18, No1, Sage Publications, Thousand Oaks, New Delhi.

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

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

Gill Martin and Spriggs Angela (2005) *Assessing the Impact of CCTV*. Home Office Research Study @www.homeoffice.gov.uk/rds/pdfs05/hors292.pdf

Goold Benjamin J (2003) *Public Area Surveillance and Police Work: The Impact of CCTV on Police Behaviour and Autonomy*. Surveillance and Society 1(2):191-203 @www.surveillance-and-society.org

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

Introna Lucus D and David Wood (2004) *Picturing Algorithmic Surveillance: The Politics of Facial Recognition Systems*, Surveillance and Society 2(2/3), 177-198.

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

Kaufman Frederick (1998) *Commission of Proceedings Involving Guy Paul Morin* @www.justice.gc.ca/en/dept/pub/hop/p3.html

Klein G (2000) Analysis of Situational Awareness from Critical Incidence Reports in DJ Garland (Ed), Situation Awareness Analysis and Measurement, pp51-71, Mahwah New Jersey, Lawrence Erlbaum Associates.

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

Lyon D (2003) *Airports as Data Filters: Converging Surveillance Systems After September 11th*.Information, Communication and Ethics in Society 1(1), pp13-20.

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

Mathews Jenny (2005) *Hi tech, High Transport Security?* BBC News, 14th November 2005 @www.news.bbc.co.uk

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

Phillips PP, Growther R, Micheals DM, Blackburn E Tabassi and JM Bone (2003), *Face Recognition Vendor Test 2002 Overview and Summary* @biometricsinstitute.org/bi/faceRecognitionVendorTest2002.pdf

Ruff HA, Narayanan S and Draper MH (2002) *Human Interaction With Levels of Automation and Decision Aid Fidelity in the Supervisory Control of Multiple Simulated Unmanned Aerial Vehicles,* Presence II(4), pp325-351.

Semple Janet (1987) *Bentham's Haunted House*. The Bentham Newsletter, 11, pp35-44.

Stahl Bernd Carsten (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).

Werrett Simon (2003) *Potemkin and the Panopticon: Samuel Bentham and the Architecture of Absolutism in Eighteenth Century Russia.* Surveillance and Society 1(2):191-203 @www.surveillance-and-society.org/articles1 (2)/publications. PDF

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