GlobalResearch
Center for Research on Globalization

Britain's Police State: London arrests based on CCTV identification. Britain adopts Chinese model of policing protest?

By Nathan Allonby
Global Research, December 21, 2010
21 December 2010

Region: Europe
Theme: Police State & Civil Rights

CCTV has led to large scale arrests, following the recent student protests in London, over increased tuition fees. A total of over 180 people have been arrested, with the majority identified by CCTV.

The current arrests very much represent a landmark – we are now equipped for the Chinese approach to public order, in almost a complete reversal previous British policing.

The power of the new system is based on the ability to track down individuals at leisure. However, this ability could be used as easily to track anyone, in "political policing" of lawful democratic activity.

More than 180 people have been arrested by police investigating rioting during the series of protests against rising student tuition fees.

Senior officers said the vast majority of the 182 suspects were aged between 17 and 25 and have never been involved in violence or criminal acts before.

Detective Chief Superintendent Matt Horne, who is leading the inquiry, said he expects the figure to grow considerably as 80 officers comb through video footage.

…

Speaking at New Scotland Yard… he said the inquiry could take months to complete. … "What struck me is the number of people arrested who did not go that day with necessarily any intention of committing any violent action."

Evening Standard, London

Police had been criticised for their handling of the protests, particularly the tactic of "kettling", where large groups – hundreds – of demonstrators were confined for several hours and not allowed to leave until late at night. It was argued that this tactic actually caused violence, and punished many who had done nothing wrong. Similar criticisms were made when this tactic was used at the G20 protests in London last year.

Here is the contrast: – previously, almost all the arrests would have taken place at the scene, to remove trouble-makers from the fray, to de-escalate the situation, not afterwards, to "settle scores". Now, everything has changed.

The combination of these two new tactics – containment and surveillance – has parallels with handling of large disturbances by Chinese authorities: – rather than attempt to make arrests at the scene, the police merely contain the disturbance to limit any damage; CCTV photography is used to identify individuals within the crowd, who are then arrested later, at their homes.

The use of CCTV in China, to identify protestors, dates from at least 1989 : –

[Box 3:] "Neutral" Technology at Tiananmen Square

Following the Tiananmen Square massacre in 1989, the Chinese authorities tortured and interrogated thousands of people in an attempt to identify the demonstration's organizers. But even if the students and workers had resisted the terrors of the secret police, the hapless demonstrators stood little chance of anonymity. Stationed throughout Tiananmen Square is a network of UK manufactured surveillance cameras, designed to monitor traffic flows and regulate congestion. These cameras recorded everything that transpired in the months leading up to the tanks rolling into the square.

In the days that followed, these images were repeatedly broadcast over Chinese state television. Virtually all the transgressors were identified in this way. Siemens Plessey, which manufactured and exported the cameras, and the World Bank, who paid for their installation, claim they never had any idea that their "technologically neutral" equipment would be used in this way. However, in 1995 the World Bank authorized the funds to set up the same traffic flow system in Lhasa, the capital of the Tibet Autonomous Region. Lhasa is not, as yet, known for having problems with traffic congestion; besides, the area in which the traffic flow system is in operation is solely for pedestrians. (56)

Is it valid to make a comparison between Britain and China? After all, the people arrested in Britain allegedly were involved in violent disorder and British government is not going to torture them.

On the other hand, the model of policing has sharply diverged from traditional "*policing by consent*", with scenes such as police horse-charging protestors and dragging a disabled man from his wheelchair. Something has to have gone wrong when police arrest, not determined trouble-makers but, large numbers of young people who "*have never been involved in violence or criminal acts before*" and "*who did not go... with... any intention of committing any violent action*".

The techniques of surveillance and identification employed here could just as easily be used to identify lawful political activists, leaving a quiet meeting. There is the manpower to do this – by comparison with the current 80-man search, Britain already has a permanent police unit of 100 staff, looking full-time for "extremists". Extremism is a term also applied to peaceful, lawful protest.

In the near future, identification is likely to be much faster and less labour-intensive, due to new CCTV technology, scheduled for implementation. Not just in Britain – New York plans soon to overtake London in CCTV technology.

There are very strong European dimensions to these events – the European wave of austerity programmes and protests, the European sponsorship of new surveillance technology and what may be an emergent European style of policing political dissent, with

an EU manual on policing public order. We can see common tactics in policing, for example, *kettling* – penning-up large numbers of demonstrators – which was used at London was also seen at the Copenhagen Climate Summit, December 2009.

Identification

How have British police identified these 182 suspects in London – people mostly without a photo on file?

One way has been to post photographs on the news, as the Chinese did in 1989, but it appears the majority were identified by other means, because the number of photos released has been small compared with the number of arrests.

A second method the police announced was by searching websites and forums, "where activists might boast about their actions".

It has not been disclosed how police have conducted this search, so this will inevitably be the subject of speculation. In theory, police could able to search social websites for photos matching suspects, using new facial recognition and *semantic search* technology. Facial recognition has made huge progress recently, largely overcoming problems with size of databases. Semantic search makes it possible to search on criteria other than text, for example, to search by image characteristics. The UK National CCTV Strategy discusses how the CCTV network may be used in conjunction with other databases to allow data-matching/mining and profiling; the same techniques can be applied to any database.

Facebook has recently added facial recognition to its features, to allow users to tag names to photos. Privacy on the Facebook scheme is opt-out, rather than opt-in, hence it is possible many people may be unaware of their participation in this new functionality. Other people may be completely unaware that there may be photos of them on the web, posted by others (e.g. group photos with friends) and tagged with their name. Although Facebook claim their tool is not suitable for site-wide trawling, the intelligence agencies have put significant resources into data-mining social network sites.

However, the most powerful tool to identify people is by tracking their movements, to a point where they can be identified, for example, by getting in a car (which can be identified by vehicle registration) or by getting on public transport (potentially to be identified by a travel pass). So that any camera can identify a vehicle, Automatic Number Plate Recognition (ANPR) facility is being added to town centre CCTV systems, not just traffic cameras, as part of the National CCTV Strategy (see p40). On public transport, the National CCTV Strategy, sought to integrate "*Transport system cameras to travel cards*"(p40), so that travellers identities could be established as they passed through barriers. Police tracking of travel cards is an established reality – in 2008, police obtained over 3000 individuals' travel records from Oyster Card, Transport for London's smart-card. OysterCard has been so successful, it is now being rolled out across the entire UK, for all public transport, as the integrated ticketing scheme.

Technology to track individuals from camera to camera, through a city's CCTV network, has been available for over a decade and has been deployed widely. More recently, technology now allows police to track suspects by their clothing. This allows police to re-acquire suspects, if they are lost between camera sightings.

...Once the item to search for is selected – a Nike T-shirt worn during a shop robbery, for instance – the computer analyses it, pixel by pixel.

It then scans for matches in the police database and footage from other CCTV cameras in the area, and provides a list of search results to help identify and locate the suspect.

"We say to the machine, 'there's a Coke logo, go and find it'," says David McIntosh, of Omniperception. "The technology is like a bloodhound. You give it a smell and it will go off looking for it."

For example a camera might only have a clear of shot this fictional Nike-clad suspect from 150 yards away. Feed this image into the system, and it will recognise the outfit filmed from other angles and distances, even if partially obscured.

The best results are gleaned from giving the computer an image of a suspect, rather than feeding it "clean" brand logos.

...
Detective Chief Inspector Mick Neville, of the new London-based unit [Visual Images, Identifications and Detections Office (Viido)] ... says the system could help track a suspect's movement before and after an offence. This may throw up footage of their face without hat or hood, or even where they live.

How can CCTV spot suspects by clothing logos?

BBC, 7 May 2008

The power of his technology is its ability to trawl through vast amounts of data, generated by extensive camera networks, or to piece-together fragmented information, which may have been assembled from numerous sources. This is important considering that the majority of the 500,000 CCTV cameras in London are not yet networked, and police have to search laboriously through recordings – for example, private CCTV systems in shops and cameras on buses. (However, it is likely that many of these cameras may become networked within the decade). It is easy to see that without machine-searching, it would be impractical to access and organise this huge amount of data.

Number of cameras, ease of access

Many quoted numbers of CCTV cameras in Britain can be misleading. Yes, there are a lot of cameras, but in London, only few of tens of thousands of these can be accessed easily by police, which would make the rest relatively useless for routine political surveillance. Those cameras that have live-networked access vary in ease of data-retrieval. Despite this, the London CCTV network provides formidable coverage, particularly on trains and the London Underground.

There had been a sustained programme to upgrade the system, under the National CCTV Strategy. This appeared to be threatened by the pledges of the new government, elected this year, but now, it seems likely that the recent disturbances will guarantee the upgrade goes ahead. The London Olympics in 2012 are also expected to prompt major upgrades of police and surveillance systems.

Although there is an official estimate of 500,000 CCTV cameras accessible by police in

London, the vast majority of these can only be accessed by requesting recordings.

In 2007, there were 10,524 local authority CCTV cameras in 32 London boroughs – but the figure today may be significantly greater – these are all networked live-feed public cameras. Additionally, there are currently 12,000 cameras on the London Underground network, plus Transport for London has 900 traffic cameras, to which the police also have networked live access.

These are still large numbers – about four times the number used by NYPD and transit.

At the present time, cameras on London buses are not networked live – however, there are "60,000 recordable CCTV cameras operating on the 8,000 London buses", and the police make "650 requests every month for images". Several other British cities, do have live-feed CCTV on buses, which can be accessed not only by central commend but also by mobile officers, on hand-held viewers. This seems likely to come to London by 2012.

Images obtained from private cameras are important. Police announced that photographs of suspects have been obtained from the private CCTV systems of shops along the route of the march. There is a voluntary registration scheme for privately-owned CCTV systems, so that the police may obtain recordings when required. As part of new proposals for regulation of CCTV, this registration is expected to become compulsory. As part of the controversial "Internet Eyes" monitoring scheme, many shops are beginning to link their CCTV systems to the internet. It is easy to see how this could evolve into live-access to the authorities.

At present, the London CCTV network still suffers from a heritage of piecemeal construction,

… In London, video from cameras is transmitted via a system comprised of several separate networks and storage points based on London's police districts and borough maps. Although CCTV pictures are also stored in London for 30 days, they are harder to retrieve on an urgent basis because of the decentralized design of the storage and transmission system, making it more time-consuming and logistically awkward to screen and assemble video chronologies in cases where trails cross network boundaries.

Mark Hosenball, Newsweek, 13 May 2010

London also had to shut-down some cameras, to enforce standardised digital formats.

The CCTV network in London is still evolving and still very piecemeal – the price of being a pioneer. This is why it has taken as many as 80 officers to track down 180 suspects. It won't be nearly so difficult in future. We can be fairly certain that, by the Olympics in 2012, the network will be much more streamlined and automated. There has been a sustained programme to create this, as part of the National CCTV Strategy. Reportedly, under an initiative called 3Ci (Command, Control, Communication and Information) access and control has now been consolidated centrally. It is believed that now, any of London's networked CCTV cameras can be accessed and "driven" from any one of three "Special Operations Centres". Several similar regional CCTV centres have now become operational throughout the UK.

Other cities, like New York, are intending to learn from London and will soon install up-to-date, efficient systems, free of the London system's limitations.

Is this about crime?

In numerous studies, CCTV has been found to have a very low effect in reducing crime.

CCTV represents a radical departure from the approach of traditional policing. The methodology of observation and recording is that of the secret policeman, not that used in tackling real crime. Perhaps that's why CCTV has had so little impact on crime, yet has been so effective at arresting demonstrators.

According to this report

…the London CCTV system is mainly useful for reconstructing crimes or incidents after they happen—rather than preventing them—people familiar with British security measures say that the camera system is gradually being used more extensively for intelligence-gathering and surveillance by undercover agencies like Special Branch, the political policing arm of Scotland Yard, and MI5, Britain's clandestine domestic intelligence service…

Mark Hosenball, Newsweek

If CCTV does not deter crime, does it help solve crime, and catch criminals? In London, CCTV does not seem to have helped much, finding the perpetrators of real crime, such as robbery and violence,

Only one crime is solved a year for every 1,000 CCTV cameras, police admitted …

Detective Chief Inspector Mick Neville said: '£500million has been spent by the Government on cameras. Despite this, in 2008 less than 1,000 crimes were solved using CCTV …'

He said that of the 269 robberies reported in one month only eight were solved with the help of CCTV footage. …

Detectives are thought to be reluctant to scour hours of recorded footage 'because it's hard work'.

CCTV helps solve just ONE crime per 1,000 as officers fail to use film as evidence

Matthew Hickley, Daily Mail 25th August 2009

In parallel with this new-found investment in technology, policing in Britain has been moving away towards something more remote and detached. Town-centre police stations, where the public could go to report a crime, a lost dog or whatever, have been closing down, to relocate out-of-town, to large "patrol bases" in business parks, which are closed to the public. It sounds like beat-policemen, community contacts and the human touch are seen as a thing of the past.

Where next?

The big problem with CCTV has always been a shortage of people, to watch the cameras, or to sift through recordings. All this is set to change with radical artificial intelligence (AI) systems currently under development by the European Union (EU). Now, machines will be able to watch the cameras, spot crime or aberrant behaviour, alert officers to the scene, track (and identify) the suspect, and collect the relevant video clips into a file, together with any other relevant information from other feeds.

HERMES, INDECT and ADABTS are AI suites aiming for deployment in 2012-3. They will be capable of analysing multiple different types of data-streams, identifying events and assembling a file with a commentary.

According to the EU website, the HERMES system will be capable of recognising events such as robberies or violence, and can

"*not only detect events in real time as they are filmed by surveillance cameras but also describe them semantically and react to them intelligently. It operates at three levels: tracking the movement of people and objects; monitoring the behaviour of people; and, in the case of high-resolution footage taken at close quarters, detecting changes in facial expression.*"

HERMES is also designed to automatically search for and correlate other data, from other sources, such as multiple alternative camera positions or other identification systems.

ADABTS is intended to recognise

"suspicious behaviour" so [this] can be automatically detected using CCTV and other surveillance methods. The system would analyse the pitch of people's voices, the way their bodies move and track individuals within crowds.

How the EU is Watching You, Open Europe, 2009 (p24)

ADABTS is being developed by a consortium including arms company BAe Systems and the Swedish Defence Research Agency.

INDECT is aimed at surveillance in a different sphere – it will enable,

"*continuous and automatic monitoring of public resources such as: web sites, discussion forums, usenet groups, file servers, p2p [peer-to-peer] networks as well as individual computer systems, building an internet-based intelligence gathering system, both active and passive* [with the aim of] *automatic … recognition of abnormal behaviour or violence*"

ibid.

Tom Burghardt described INDECT as a system for "profiling internet dissent" INDECT had emerged from strategies in Europe and the CIA to data-mine information about political opposition, from social networks and related sources.

What these official descriptions above do not mention is that, to do their job, these systems have to lead to the automatic machine-identification of individuals. It is not hard to see how the ability to track individuals and access "multi-media data streams" will make this possible. It is also easy to see how the ability to identify individuals combined with the ability to assemble data in organised files, with notes, could construct personal dossiers on the movements and contacts of any individual. This would be a gift for the surveillance and control of legitimate political activity.

In 2007, a European Union working group presented a proposal called the "Digital Tsunami", to track and record the lives of every individual. This was described by Tony Bunyan of Statewatch: –

“Every object the individual uses, every transaction they make and almost everywhere they go will create a detailed digital record. This will generate a wealth of information for public security organisations”, leading to behaviour being predicted and assessed by “machines” (their term) which will issue orders to officers on the spot. The proposal presages the mass gathering of personal data on travel, bank details, mobile phone locations, health records, internet usage, criminal records however minor, fingerprints and digital pictures that can be data-mined and applied to different scenario – boarding a plane, behaviour on the Tube or taking part in a protest.

‘The surveillance society is an EU-wide issue’,

Tony Bunyan, 28 May 2009, The Guardian

Officially, this proposal was never adopted as policy. In practice, every measure within it *has* been adopted, under the new name “Digital Agenda“. Worryingly, this dovetails with a new, authoritarian approach in the “Stockholm Programme” on security, justice and home affairs.

CCTV becomes much more powerful in this role when combined with complimentary tracking technologies, such as the RFID chips (Radio-Frequency Identification), which have been inserted into ID cards around the world. Bank cards too increasingly incorporate RFID. In several European countries, bank cards have taken on the function of ID cards – called eID (or “electronic signatures“), issued in collaboration with the national population register, via “commercial certification authorities“, they are recognised for accessing public services. As mobile phones are becoming used for payment, these too are being registered within the same system. This international eID registration system has come about to enable electronic payment, and has been organised by a UN agency, UNCITRAL. This has become another branch of a global population register.

Technologies exist to locate and identify the position of all RFID tags within the view of a CCTV camera. Integration is becoming simpler and more affordable, with commercial solutions available.

Since opening in 2007, all passengers at Heathrow, Terminal 5 have been tracked and managed by a combination of RFID and facial recognition CCTV. The system was developed by the European Union as “The INtelligent Airport” project (TINA). Normally at airports, domestic and international passengers would be carefully segregated, for security, but at Terminal 5 they are allowed to mix in one departure lounge, controlled by ubiquitous surveillance. Effectively, passengers are tracked by RFID and facial recognition CCTV is used to verify, to a high degree of accuracy, that the subject is the authorised holder. The system can also identify anyone not carrying an RFID pass, and recognise a pass dropped on the floor. The system can also recognise the RFID in passengers’ passports, which are the same as RFID in national ID cards, both standardised by the ICAO. This surveillance system is trusted to provide the same level of security as physical segregation. Facial recognition is now a proven, mature technology.

The European Union is investing heavily in promoting RFID and a system for tracking RFID, called the Internet of Things (IoT). Every tagged object will have its own webpage, with the web-address being its RFID serial number. Every time an RFID tag is scanned, the webpage will be updated with the time and location. Designed to track goods in the supply chain, corporations realised that this could also track customers after purchase, to produce marketing information. This scanning and logging will become frequent and pervasive, as

RFID scanners replace anti-theft portals at shop entrances, and all will be networked into the Internet of Things.

It is easy to see how the Internet of Things could potentially dovetail with intelligent CCTV and AI systems to enable ubiquitous surveillance.

Conclusion

The real threat comes not from CCTV but from its application to identifying citizens, then tracking and recording their lives. This phase of CCTV is only just beginning, but will be heavily upon us, very soon.

We can get a glimpse of this in China, as described by Naomi Klein:

Chinese citizens will be watched around the clock through networked CCTV cameras ... Their movements will be tracked through national ID cards with scannable computer chips and photos that are instantly uploaded to police databases and linked to their holder's personal data. This is the most important element of all: linking all these tools together in a massive, searchable database of names, photos, residency information, work history and biometric data. When Golden Shield is finished, there will be a photo in those databases for every person in China: 1.3 billion faces.

China's All-Seeing Eye

Naomi Klein, May 14th, 2008, Rolling Stone

Authors such as Naomi Klein and Greg Walton have pointed out the role of the West in supplying this surveillance technology to China. Our governments have shown no moral scruples and far too much interest in this convenient field-trial of repression.

If we can't trust the morality or ethics of our governments, can we really trust them with the enormous power they are assembling?

(For more information on surveillance cameras visit the No CCTV website at www.no-cctv.org.uk)

Articles by: Nathan Allonby