the police foundation
improving policing for the benefit of the public

8 September 2008

Oxford Policing Policy Forum

Too much Surveillance?

Report of the fifth Oxford Policing Policy Forum.

All Souls College,
Oxford

The Oxford Policing Policy Forum

The Oxford Policing Policy Forum is a joint initiative of the Police Foundation and the Centre for Criminology at the University of Oxford. The forum provides an opportunity for a wide range of stakeholders interested in policing to discuss fundamental issues under Chatham House rules. The main purpose is to encourage informal debate rather than inviting an audience to listen to formal presentations. Participation is by invitation only (see guest list).

This meeting of the Forum was chaired by Roger Graef and an introductory presentation setting out some key issues was given by the Rt Hon Keith Vaz MP of the Home Affairs Select Committee (HASC). The afternoon session commenced with a presentation from
Professor Mark Nixon of the School of Electronics and Computer Science at Southampton University on his current research on gait recognition.

Background

In November 2006 the Information Commissioner Richard Thomas stated “Two years ago I warned that we were in danger of sleepwalking into a surveillance society. Today I fear that we are in fact waking up to a surveillance society that is already all around us[1].” In 1993 CCTV cameras captured the image of James Bulger being led away by two boys and over the following decade the Government and British society seemed to regard CCTV as the answer to a wide range of crime and disorder problems. Today there are 4.2 million CCTV cameras in Britain, one for every 14 people and despite numerous studies in CCTV, there is no hard evidence that the cameras significantly reduce any crime other than vehicle crime.

The thirst for other forms of surveillance including the DNA database, identity cards and the monitoring of telephone, email and post, has been steadily increasing. By the time of the Olympics in 2012 hand held police computers will be able to take fingerprints, access CCTV images and download records from the police national computer. The Communications Data Bill is due to come before Parliament shortly, aiming to create a database of all telephone calls, emails and internet use by UK citizens. The Information Commissioner’s Office has expressed concern over whether such a Bill is justified, proportionate or desirable and whether there will be adequate safeguards in place.

The fifth Oxford Policing Policy Forum posed the question ‘Too Much Surveillance?’ and aimed to stimulate discussion about the ubiquitous use of various forms of surveillance technology in the UK, particularly CCTV, the interception of electronic communications, the DNA database and national identity cards. The Forum debated what an acceptable limit to the use of such technology might be, whether we have reached that point and if so, what might be done to halt the spread. Just because society now has the technological capacity to monitor every person in society does this mean it should do so? How much surveillance is too much and when would we know that we’d reached that point?

The report of the Home Affairs Select Committee

In June 2008, the HASC published a detailed report into surveillance called ‘A Surveillance Society.[2]’ The Rt Hon Keith Vaz MP, Chair of the HASC, addressed the Forum, sharing his views on some of the issues it raised. The report rejected the notion that Britain is a surveillance society but expressed grave concern over the security and safety of how gathered information is stored. There are regular losses of data from private companies and government departments, such as the data held on the Police

[1] press release Information Commissioner’s Office 2 November 2006

[2] http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/5802.htm

National Computer that was recently mislaid by PA Consulting; the discovery of a memory stick containing details of troop movements from the Ministry of Defence on a nightclub floor; nine separate incidents of data lost from the Ministry of Justice; and the loss of child benefit data. This systemic failure to keep information safe is of great concern to the government and the public and needs to be more effectively addressed.

The Committee's report recommended moving towards 'data minimalisation' – collecting only necessary data and storing it for the shortest period of time. So for example currently, on arrest, a suspect's data is taken and logged on the Police National Computer, but even if the suspect is not subsequently charged, the data remains on the database, ostensibly in case of any future crime. Meg Hillier MP, Under-Secretary of State for the Home Office, stated in her evidence to the HASC that the storage of DNA was vital to police work. However, a proper case has not been made for the need to store the personal details of those who are not charged with committing an offence. Once a citizen's personal details are held on the police national computer, it is extremely difficult to get those details removed, whether charges are laid or not.

A second issue raised by Mr Vaz concerned the regulation of surveillance. Who is responsible for watching over those who watch over us? To whom do the public turn if something goes wrong? In principle, the Information Commissioner has been given this remit, but in practice he does not have anything like the resources (let alone the necessary powers) to do so effectively. The HASC heard evidence that 80% of film captured on CCTV camera is of such poor quality that it is virtually unusable. So, for example, whilst the images of the two boys who abducted and then tragically killed James Bulger have been indelibly imprinted on the public's mind, their faces were actually not visible (and so they were not identifiable) as they were walking away from camera. Furthermore, evidence caught on camera is sometimes not viewed for months.

Surveillance, Mr Vaz concluded, is here to stay, but it must be used appropriately and efficiently and be subject to effective regulation. The use of surveillance must be fully justified and the reasons must be transparent and explained if the right balance is to be struck between security and liberty. Big brother needs to become an uncle not an enemy.

Data loss

The Forum expressed universal unease over the regular leaks and loss of data from both government departments and private organisations. One suggestion to curb this problem was to invoke criminal sanctions, but this was dismissed on the grounds that the level of criminal intent or negligence required to justify a prosecution would be too high. In the majority of cases, data is accidentally lost by a low level employee and holding either him, his manager or even the head of his organisation criminally liable was also considered excessive and unlikely to deter others since most data loss is accidental, not intentional.

It was suggested that there was an urgent need to increase the security procedures for holding personal data, such as using encryption or making it harder to download data onto portable devices such as memory sticks, to guard against its misuse if lost or stolen. Slowing down information transfer might also help to improve data security. The Forum voiced concern about the Government's plan to continue with the development of ID cards without having ensured a safe and reliable data storage system.

There is a further issue of the intentional extraction of data for fraudulent purposes. Databases are extremely valuable and the information they contain can potentially be misused for financial or social gain. Where data is held on behalf of the government or the police by private sector companies, adequate safeguards must be in place to ensure that the information is protected.

Function Creep

Participants highlighted the steadily growing use of gathered data for additional purposes, known as 'function creep'. When new surveillance legislation is brought before Parliament, it is often justified on the basis that additional powers are needed to fight terrorism and serious and organised crime. There is a danger, however, that over time, greater use is made of such powers by third parties. In 2000, the government passed the Regulation of Investigatory Powers Act in 2000, but the powers conferred by this legislation are being used by local councils and other non-governmental bodies for purposes other than those for which they were intended (e.g. to detect and punish relatively minor crimes such as fly tipping or to check whether parents reside in the appropriate school catchment area).

The private sector must bear some responsibility for the rapid growth of surveillance. Information collection is now a very profitable commercial enterprise and the commercial sector has not been slow to exploit the profitable opportunities that new technology often presents. Systems such as fingerprint recognition for checking whether pupils are entitled to free school meals may soon become commonplace. Greater care must be taken before third parties are given the authorisation to use powers passed by Parliament to improve the security of the nation but that affect the liberty of the individual citizen. Increasing incursions into individual civil liberties can eventually lead to a public backlash, which may in turn make the government's job of securing the nation's security more rather than less difficult.

Data Minimalisation

The HASC heard evidence from the police that CCTV is a vital tool in the prevention and detection of crime. The Forum agreed that there must be sound reasons to take and retain personal data, that only data that is really needed should be collected and that it should be stored for the shortest amount of time possible. Identity cards, for example, do not need to state a person's age but merely whether someone is under or over the age of 18.

Data that is no longer required should be destroyed and a simple and transparent system needs to be put in place to ensure this happens. When personal data is taken in error or when mistakes in the data occur, it takes an inordinately long time to correct any such errors. There seems to be no justification for holding a person's DNA following their arrest if no charges are laid (as with fingerprints) and the view of the Forum was that such data should be automatically removed from the Police National Computer with the person concerned receiving written confirmation that this has been undertaken. The current system, which allows suspects who have not been charged to apply to have their data removed (whether DNA or fingerprint) is time consuming, rarely results in removal and should be reviewed where charges are not laid.

The time limit for police storage of CCTV images varies from force to force and is between 1 and 16 months. There is a need to determine a standardised time period, which should be as short as possible.

Anti-Social Behaviour

The Forum raised an issue previously discussed in the Fourth Oxford Policing Policy Forum on the growth of police powers, namely the need to find a way to deal with anti-social behaviour without automatic recourse to the law. The erection of CCTV cameras and the retention of data were not seen as effective solutions to Britain's anti-social behaviour problems. One review of research on the effectiveness of CCTV found that cameras reduce crime by no more than 5%, whereas better street lighting reduces crime by 20%[3]. CCTV is expensive and as yet there seems to be no compelling evidence that it significantly reduces crime or anti-social behaviour.

Surveillance and Society

The Forum posed the question 'how much surveillance is too much?' and participants were invited to also consider this in terms of its potential impact on society as a whole. The point was raised that Britain has become a voyeuristic society – one of reality television, mobile phone cameras and the internet. There was concern that users of internet sites such as Facebook (predominantly the young) do not understand how to ensure their data is kept private nor the potentially adverse consequences of data sharing. The point was made that although young people are internet wise, they are not internet savvy and many do not realise how public their internet use is. The search engine Google stores use of its site including pages visited, YouTube videos viewed and a unique hard disk identifying number. The US government ordered Google to hand over a proportion of this information in order to assist with its fight against pornography. There is a need to help people engage with and understand these issues more.

By contrast, the public seems to be much more wary of the NHS database. There is a real reluctance to allow personal health details to be stored nationally on a system that could be hacked or misused. The Big Opt Out Campaign has prompted large numbers of people to request the exclusion of their personal documents[4] from the NHS database and a BMA survey found nine out of ten doctors have no confidence in the system[5].

There are signs that public opinion on the use of CCTV has begun to shift. In the 1990's, the public saw CCTV as a solution to crime and anti-social behaviour and the notion that 'if you have nothing to hide then you have nothing to fear' was fostered. However, attitudes towards CCTV are changing, with people more suspicious of the effectiveness of CCTV and the storage of personal data.

The effect of surveillance on marginal populations was highlighted as an area of particular concern. Some members of society are subjected to surveillance and data gathering more than others. 37% of black men in England and Wales have their profiles on the DNA database compared with 1% of white men. There are fears in the black community that youths and victims are not reporting crime due to a desire to avoid their data being retained, and concern that once they are known to the police, they are more likely to be targeted, harassed or arrested. The Forum also expressed unease over data profiling, where DNA is analysed and compiled to see whether statistical trends appear. The DNA database provides an enormous pool of samples, which could potentially be used or misused for a range of research and other purposes.

There is a danger that too much surveillance actually undermines trust in the state and its associated agencies. Trust is critical to good police-community relations and ultimately the legitimacy of the police. The relationship between the police, the individual and the state is important and the more the state

[3] Armitage, Rachel (2002) *To CCTV or not to CCTV? A Review of current research into the effectiveness of CCTV systems in reducing crime:* Nacro, May 2002

[4] ' Revolt as 200,000 people demand to opt out of new NHS database scheme' Daily Mail 31 December 2007.

[5] BMA News Press Release 1 Feb 2008

intervenes in the personal lives of the citizen, the greater the danger that he/she will withdraw their consent. Too much surveillance is likely to invoke suspicion and distrust and encourage people to withdraw such consent. The 1990's saw the evolution of the 'Hoodie', an item of clothing which obscures part of the wearer's face. Hoodies quickly became associated with young people involved in crime and anti-social behaviour who used them to obscure their identity from CCTV cameras. Today the Hoodie has become a powerful symbol with hooded teenagers feared by the public, whether involved in illegal activity or not. There are now cases where citizens have turned the camera on the police, using mobile telephones to photograph them, resulting in being ordered to delete the photographs or even being arrested for assault[6]. These examples suggest that there must come a point when society is so saturated with surveillance it becomes counter-productive. The critical issue is to know when this occurs and be able to stop it.

The huge commercial profits that can be made from surveillance cameras has understandably led to the corporate sector investing in ever more sophisticated technology. The expansion of surveillance in general and the growth of CCTV cameras in particular has therefore been as much due to commercial interest as executive decision. Large corporations are able to influence the amount and quality of CCTV in society and they do so often without any consideration of the impact it may have on wider society. When considering surveillance and its effect on society it is therefore no longer sufficient to simply view this as a matter of achieving the right relationship between the individual and the state, which in this case is heavily mediated by powerful corporate interests.

Regulation

The Forum commented on the need for greater regulation of surveillance powers. The technology in this field advances at a far greater rate than the law. In the US, the law took 100 years to catch up with intercept technology; in the UK it took 300 years. Furthermore the current surveillance legislation such as the Regulation of Investigatory Powers Act 2000 is complex and confusing. The Communications Data Bill will allow for wide reaching surveillance and if a database of all telephone, email and internet use is to be established, the public needs to be able to trust those who hold such data and be reassured that they are subject to effective regulation and held to account for any failings. Concerns were raised, however, that existing resources and procedures for regulating information collection, storage and transfer are inadequate. In addition to effective regulation, adequate safeguards are needed to ensure that if a future malevolent government comes to power, or the country is invaded, personal databases cannot fall into the wrong hands or be used for unacceptable purposes, as happened during the Second World War when Hitler invaded the Netherlands.

In the UK a warrant for the interception of a telephone line is granted by the Home Secretary – a politician. This contrasts with many other countries, such as the US, where the decision is in the hands of a judge – an independent figure. The Forum queried whether an executive would be in a sufficiently neutral position to authorise the interception of a person's communication.

There are also practical issues with the regulation of information. By 2016, it is predicted that there will be 450,000 million communication events in the UK per year. This is a staggering number and the government simply does not have the time or the resources to effectively monitor them. Such issues need to be confronted now rather than in 2016, by which time it may well be too late.

[6] 'Man arrested and locked up for five hours after taking photo of police van ignoring 'no entry' sign' Daily Mail 20 August 2008

The Future

CCTV is a fast growing commercial industry, with predictions that the CCTV economy will increase by 10% in the UK in the run up to the London 2012 Olympics. In China, experts say the industry will be worth more than £21 billion by 2010 (up from £250 million in 2003)[7] and CCTV companies, keen for a slice of the profit, are testing the limits of their systems in China. Surveillance technology is becoming ever more sophisticated, and 'trigger' events such as the London bombings or the Olympics, only help to drive such technology to new heights.

Professor Mark Nixon gave us a glimpse of the future in his presentation to the Forum on the development of gait recognition. The School of Electronics and Computer Science at Southampton University and Information Signals Images Systems are working in partnership to develop a system where a computer would analyse a person's shape, build and step. This data could then be used as part of a 'walking identity parade' to identify a suspect from their gait, which people apparently find much easier than facial recognition. Other technological developments planned for the future include, by 2012, hand held police computers that will be able to take fingerprints, access CCTV images and download records from the Police National Computer.

The Forum posed the question – just because we have the technology, should we use it? As technology advances and its uses are commercially exploited, it becomes the default or at least preferred solution to a wide range of problems, including some for which the technology was never intended. It soon becomes a systemic way of life that is hard to dismantle and from which it is difficult to retreat. The Forum concluded that further research should be conducted on the cost-effectiveness of CCTV and its derivatives before additional funds are spent.

Conclusion

The Fifth Oxford Policing Policy Forum identified a number of fundamental issues and concerns. Surveillance in Britain has steadily increased without adequate public understanding or debate. Britain is in danger of becoming a society where everyone is effectively 'on parole', and this without sufficient exploration of the political and social consequences of the spread of surveillance. There was understandable pressure on the security services to prevent and detect planned terrorist activity and serious and organised crime and a real need to provide those services with the means to do so. However, access to surveillance data is being given to third parties who are using it for increasingly spurious purposes.

The Forum decided it was the collection rather than the use of personal data that posed the greatest threat to individual freedoms. Data will always be lost, sold or used for other purposes. Fraud will always be a temptation and hackers always find ways to achieve their ends. The risks can be lessened by minimising the amount of data that is collected and the length of time it is stored and by not relying solely on yet further technological solutions – encryption for example – to do so.

How much is too much? The Forum acknowledged this was a difficult question to answer and that, by the time society realised there was too much surveillance, it may be too late. It is always difficult to strike the right balance between security and liberty, but what would seem to matter most is that those in power are continually challenged to ask themselves whether and when enough becomes too much.

Abie Longstaff, September 2008

[7] 'Profit from Big Brother's embrace of the Olympics' Money Week 25 June 2008