# Surveillance: who's really in control?

**Abie Longstaff** and **John Graham** point to the problems created by the increasing involvement of corporations in the surveillance society.

***The use of reasonable, proportionate and well-regulated surveillance is an essential tool in the armoury of the police and security services. Increasingly, however, the regulation of surveillance, which must take account of the right of citizens to a private life, is being subjugated to the interests not so much of the state, but of a third party – the corporate sector. Many of the advances in surveillance technology have been pioneered by the private sector with the government its principal customer, but their interests do not always coincide and there are dangers in using systems advanced by commercially interested parties without assessing their potential impact not just on the rights and freedoms of citizens but also on society as a whole.***

Given the degree to which we are now saturated in surveillance of one kind or another, is it time to take stock of the wider impact this is having on society – its values, its relationships, its hopes and its fears? In doing so, is it time to take a closer look at the existing system of checks and balances on not just the state as the main user of such technology, but also the corporate sector as the main supplier? This article looks at the regulation and control of the commercially and politically driven expansion of surveillance and asks whether anyone is really in control.

The expansion of surveillance can be traced back to the beginning of the 1990s when politicians began to embrace the politics of law and order. In 1993 dramatic CCTV images of Jamie Bulger being led away to his death by two young boys helped to convince the government and the public that the expansion of surveillance (and the use of CCTV in particular) could become the new panacea in the fight against crime. A culture of surveillance as a friendly big brother began to form based on the premise that 'if you have nothing to hide, you have nothing to fear'. Surveillance technology spread to other areas beyond security, reaching into the leisure and communications industry, particularly television (e.g. Big Brother) and the internet (e.g. Facebook and LinkedIn). The boundaries between the private and the public began to blur as young people in particular embraced new technology with little thought to any potential adverse consequences.

As the demand for surveillance grew, forward thinking entrepreneurs began to capitalise on the industry's rising market value. After the World Trade Centre bombings in September 2001, as most stocks dropped dramatically in value, those of surveillance sector companies, particularly biometrics firms, soared (Rosen, 2001). In the run up to the Beijing Olympics China invested heavily in surveillance systems, allowing corporations to develop and market surveillance equipment relatively unchecked and largely at tax payer expense (Klein, 2008). Today, technological advances in communications and surveillance have created global systems whereby citizens can be tracked by satellites, watched by cameras, monitored through identity, store or credit cards and identified via their DNA or even their gait.

Over the same period, government has increasingly made use of the private sector to perform public sector functions – areas from transport to education have been outsourced to commercial companies. So too has it made use of the commercial sector to attempt to solve the problems of crime and anti-social behaviour and to disrupt terrorism, investing large amounts of money in the research, development and application of surveillance systems such as CCTV, Automated Number Plate Recognition and biometric intelligence. However, there has been little research into how effective these new technologies are in tackling crime – the findings of what little research has been conducted are at best equivocal – let alone what their long-term effect on society might be.

Parallels can be drawn with the financial sector. Despite repeated warnings from economists, a largely unregulated banking industry was allowed to grow unchecked by the executive leading to a global economic crisis, the full effects of which are still to be felt. Similarly, the growth of surveillance is beginning to take its toll on society (Information Commissioner's Office, 2006) and allowing the corporate sector to promote the newest technology to a government eager to convince the public that they are winning the fight against crime without a full understanding of its potential down-side is a matter for real concern. As Klein points out, the more we distrust and fear one another, the more we buy surveillance systems and the more the corporations profit from them (Klein, 2008).

Corporations have become powerful global forces that control and shape our culture and our future. But unlike government, they are not accountable to the public (via parliament), but rather only to their shareholders. They have no inherent social responsibility to protect our rights and freedoms and indeed their interests may directly conflict with those of society as a whole. In setting up organisations like the Office of the Surveillance Commissioner (OSC) and the Information Commissioner's



DOI: 10.1080/09627250902904460

Office (ICO), the government tacitly acknowledges the importance of regulating and scrutinising the ways in which such technology impacts on society, but both the legislation and the resources to implement it are lacking and the bodies have been criticised for their lack of public accountability and lack of transparency (Crossman et al., 2007).

Without adequate controls, it is easy to see how commercially driven surveillance systems increase incrementally, habitualising people to their presence and well beyond the point at which dismantling them becomes feasible. Legislation to govern and regulate the surveillance industry has been slow to catch up with the technological advancements that have been achieved and continues to struggle to keep pace as the systems move on. The Regulation of Investigatory Powers Act (RIPA) and the Human Rights Act only came into force in 2000, prior to which there was only an ad hoc jumble of laws regulating surveillance.

Although RIPA was enacted to formalise and modernise the legislation in this field, it has been much criticised (see for example Bingham, 2004; Blunkett, 2004) as a complex and confusing piece of legislation. It places control of the industry not with the impartial, independent judiciary, but with the executive. It allows the Home Secretary to grant a warrant to intercept all communications from a person or premises, unlike in the US where permission is granted by a judge.

So what is to be done?

Firstly, regulation and control of the surveillance industry could be improved. Greater power could be given to the judiciary so that warrants could be granted by magistrates or judges (rather than the Home Secretary) and be subject to judicial review. The recent House of Lords Constitution Committee report, 'Surveillance: Citizens and the State' makes recommendations which are a step towards this; granting greater powers to the Information Commissioner to sanction data controllers who deliberately or recklessly breach data protection principles and a requirement that the government consult the Commissioner on any new legislation which involves surveillance. The report also invites consideration of whether local authorities are appropriate bodies to use RIPA powers.

Secondly, new surveillance technology could be more carefully scrutinised. The Home Affairs Select Committee (HASC) in its report, 'A Surveillance Society' has already recommended that only personal data considered necessary is collected and that such data should be kept for the shortest amount of time possible. To ensure personal data is kept safely – especially in light of the frequency with which data is 'lost' – higher levels of encryption and better security needs to be developed.

It may again be useful here to refer to the financial sector, where the government has had to respond speedily with a wave of new measures designed to ensure banks assess and calculate a greater range of risks. A similar line appears to be being considered for surveillance. The House of Lords has recommended a 'Privacy Impact Assessment' prior to the adoption of new surveillance schemes. This is a useful initiative, but there is a need for broader consideration of the potential impact of new surveillance technology not just in terms of its impact on people's rights and freedoms but also on society as a whole, looking at the personal and social consequences of each new scheme.

Thirdly, there is a need for wider public debate and better education about the potential dangers of too much, or too intrusive surveillance. Young people are perhaps less aware than adults of how and when they should keep their details private and why this matters. During the 1990s the public was persuaded by government that surveillance was the answer to all levels of crime and anti-social behaviour. Public opinion on this has begun to shift with strong opposition to identity cards and concerns about the storage of DNA, particularly concerning ethnic minorities.

Methods of watching people, storing data and analysing information have changed beyond all recognition in the last decade. These new techniques have automated many actions, allowing for speedier and simpler monitoring of individuals and it is perhaps no surprise to find that government is keen to use these techniques to fight serious crime and combat terrorism. However, careful and considered judgments should now be made before governments adopt new surveillance technology. The needs of the individual need to be protected not just from the interests of the state's security services, which tend to favour ever greater levels of surveillance, but also the interests of the corporate sector engaged in manufacturing and marketing increasingly sophisticated forms of surveillance technology to a state that promises ever higher levels of public protection. With the proper level of control and regulation, society can make good use of exciting commercial advances for its own improvement, but the benefits will only outweigh the disadvantages if we get the balance of interests between the state, the individual and the commercial sector right. ■

**Abie Longstaff** is a non-practising barrister and Policy Analyst at the Police Foundation. **John Graham** is Director of the Police Foundation.

## References

Lord Bingham (2004), Attorney General's Reference (No.5 of 2002) [2004], House of Lords, London.

Blunkett, D. (2004), Speech to the Police Superintendents' Association's Annual Conference. Police Superintendent's Association Annual Conference, Warwick 14 September.

Information Commissioner's Office (2006), 'A Report on the Surveillance Society', London: ICO.

Klein, N. (2008), 'Under Surveillance: Q&A with Naomi Klein', *Rolling Stone*, 29 May.

Crossman, G., Kitchen, H., Kuna, R., Skrein, M and Russell, J. (2007), *Overlooked: Surveillance and Personal Privacy in Modern Britain*, London: Liberty.

Rosen, J. (2001), 'Being Watched A Cautionary Tale for a New Age of Surveillance', *The New York Times*, 7 October.