URL: < http://privacy.openflows.org/pdf/lyon_paper.pdf >

Paper given at the Privacy Lecture Series < http://privacy.openflows.org > on November 12, 2001

David Lyon

Professor, Queen's University

TERRORISM AND SURVEILLANCE:
SECURITY, FREEDOM, AND JUSTICE AFTER SEPTEMBER 11 2001

The September 11 2001 terrorist attacks on New York and Washington prompted a series of responses from military retaliation on the country harbouring Osama Bin Laden to extensive anti-terrorist legislation aimed at domestic protection. One of the most prominent ongoing reactions is to enhance surveillance operations on a number of fronts and there has been no lack of proposals concerning the best way to achieve this. Public money is being poured into policing and security services, and high-tech companies are falling over themselves to offer not just 'heartfelt condolences' for the attack victims but technical fixes to prevent such attacks from happening again.[i]

Sociologically, this raises many important and urgent questions. With surveillance, as in many other areas, it is frequently suggested that 'everything has changed', an idea that is bound to stir the hairs on the back of any sociologist's neck. This sometimes reduces to a list of new gizmos on the everyday landscape, like iris scanners at airports, closed circuit television (CCTV) cameras on downtown streets

[i] This may be seen on many web sites, e.g. www.viisage.com

and squares, and so on, or it can refer to a 'new era' of political control that overrides previous legal restrictions on monitoring citizens. So, has everything changed, or not? I shall argue that the answer is yes and no. The underlying continuities in surveillance are at least as significant as the altered circumstances following September 11.

Focussing on the aftermath of September 11 is a worthwhile reminder that big events do make a difference in the social world. As Philip Abrams wisely said, an event ' is a portentous outcome; it is a transformation device between past and future; it has eventuated from the past and signifies for the future'.[ii] To see events -- and what I examine here, their aftermath -- as sociologically important rescues our experiences in time from being merely moments in a meaningless flux. But the event is also, says Abrams, an 'indispensable prism through which social structure and process may be seen'.[iii]

To take a notorious example, figures such as Hannah Arendt and, perhaps more sociologically, Zygmunt Bauman,[iv] have helpfully viewed the Holocaust as revealing not merely the human capacity for evil but also some of the key traits of modernity itself. The triumph of meticulous rational organization is poignantly and perversely seen in the death camp, making this not just an inexplicable aberration from 'modern civilization' but one of its products. The reason that this example springs to mind in the present context is that today's forms and practices of surveillance, too, are products of modernity, and thus carry a similar ambivalence.

[ii] Philip Abrams, *Historical Sociology* (Shepton Mallet UK: Open Books, 1982) p.191.

[iii] Abrams, p. 192.

[iv] Zygmunt Bauman, *Modernity and the Holocaust*, (Oxford and Malden MA: Blackwell, 1987).

So what aspects of social structure and process may be seen through the prism of surveillance responses to September 11? I suggest that the prism helps to sharpen our focus on two matters in particular: One, the expanding range of already existing range of surveillance processes and practices that circumscribe and help to shape our social existence. Two, the tendency to rely on technological enhancements to surveillance systems (even when it is unclear that they work or that they address the problem they are established to answer). However, concentrating on these two items is intended only to mitigate claims that 'everything has changed' in the surveillance realm, not to suggest that nothing has changed. Indeed, I think it safe to suggest that the intensity and the centralization of surveillance in Western countries is increasing dramatically as a result of September 11.

The visible signs of putative changes in surveillance have both legal and technical aspects. The USA and several other countries have passed legislation intended to tighten security, to give police and intelligence services greater powers, and to permit faster political responses to terrorist attacks.[v] In order to make it easier find (and to arrest) people suspected of terrorism, typically, some limitations on wiretaps have not only been lifted but also extended to the interception of e-mail and to Internet clickstream monitoring. In Canada (where I write) the Communications Security Establishment will be able to gather intelligence on terrorist groups, probably using 'profiling' methods to track racial and national

[v] The USA's PATRIOT Act was first, in October 2001, followed quickly by similar legislation in the UK and Canada (the Anti-terrorism Bill C-36; not yet law at the time of writing). Other countries had second thoughts on legislation as a result of September 11. In Germany, the draft of a new, more liberal immigration law was scrapped at the same time as laws regulating freedom of movement and requiring fingerprints in identity cards were tightened. See www.nytimes.com/2001/10/01/international/europe/01GERM.html

origins as well as travel movements and financial transactions. Several countries have proposed new national identification card systems, some involving biometric devices or programmable chips.

Some have questioned how new, while others have questioned how necessary, are the measures that have been fast-tracked through the legislative process. Sceptics point to the well-established UKUSA intelligence gathering agreement, for example, and to the massive message interception system once known as CARNIVORE, that already filtered millions of ordinary international e-mail, fax, and phone messages long before September 11. Debates have occurred over how long the legal measures will be in force – the USA has a 'sunset clause' that phases out the anti-terrorist law after a period of five years – but few have denied the perceived need for at least some strengthened legal framework to deal with terrorist threats.

In some respects bound up with legal issues, and in others, independently, 'technical' responses to September 11 have also proliferated. High-tech companies, waiting in the wings for the opportunity to launch their products, saw September 11 providing just the platform they needed. Not surprisingly, almost all the 'experts' on whom the media call for comment are representatives of companies. Thus, for instance, Michael G. Cherkasky, president of a security firm, Kroll, suggested that 'every American could be given a "smart card" so, as they go into an airport or anywhere, we know exactly who they are'[vi] Or in a celebrated case, Larry Ellison, president of the Silicon Valley company Oracle, offered the US government free smart card software for a national ID system.[vii] What a

[vi] www.nytimes.com/2001/09/18/national/18RULE.html

[vii] www.siliconvalley.com/cgi-bin/

commercial coup that would be! He failed to explain, of course, what price would be charged for each access to the Oracle database, or the roll-out price-tag on a national smart card identifier.

Other technical surveillance-related responses to September 11 include iris-scans at airports -- now installed at Schipol, Amsterdam, and being implemented elsewhere as well; CCTV cameras in public places, enhanced if possible with facial recognition capacities such as the Mandrake system in Newham, south London; and DNA databanks to store genetic information capable of identifying known terrorists. Although given their potential for negative social consequences[viii] there is a lamentable lack of informed sociological comment on these far-reaching developments, where such analyses are available they suggest several things. One, these technologies may be tried but not tested. That is, it is not clear that they work with the kind of precision that is required and thus they may not achieve the ends intended. Two, they are likely to have unintended consequences that include reinforcing forms of social division and exclusion.

A third and larger dimension of the technological aspect of surveillance practices is that seeking superior technologies appears as a primary goal. No matter that the original terrorism involved reliance on relatively aged technologies – jet aircraft of a type that have been around for 30 years, sharp knives, and so on – it is assumed that high-tech solutions are called for. Moreover, the kinds of technologies sought – iris scans, face-recognition, smart cards, biometrics, DNA -- rely heavily on the

[viii] See e.g. the debate over iris scans at airports, prompted by the American Civil Liberties Union (ACLU) but extending much more broadly as well. Www.aclu.org/features/f110101a.html
www.siliconvalley.com/docs/hottopics/attack/image101801.htm
http://sg.news.yahoo.com/011102/12/lne83.html

use of searchable databases, with the aim of anticipating, pre-empting, preventing acts of terrorism by isolating in advance potential perpetrators. I shall return to this in a moment, but here it is merely worth noting that Jacques Ellul's concept of *la technique*, a relentless cultural commitment to technological progress via ever-augmented means seems (despite his detractors) to be at least relevant.[ix]

So, what do these post-September 11 surveillance developments mean, sociologically? Before that date, surveillance studies seemed to be moving away from more conventional concerns with a bureaucratic understanding of power relations[x] that in fact owes as much to George Orwell as to Max Weber. This puts fairly high premium on seeing surveillance as a means to centralised power as exemplified in the fictional figure of Big Brother – the trope that still dominates many scholarly as well as popular treatments of the theme. Although some significant studies, especially those located in labour process arguments about workplace monitoring and supervision, see surveillance as a class weapon,[xi] this view is often supplemented with a more Foucaldian one in which the Panopticon plays a part.

Within the latter there is a variety of views, giving rise to a lively but sporadic debate.[xii] One fault-line lies between those who focus on the 'unseen observer' in

[ix] Knowledge of Ellul's work is often limited only to the allegedly deterministic *The Technological Society* (New York: Vintage, 1964). But he saw his sociological work as integrated with his more theological writings that are anything but deterministic. It is misleading to see his most famous work out of the context of the whole corpus.

[x] See e.g. Christopher Dandeker, *Surveillance Power and Modernity*, (Cambridge: Polity Press, 1990).

[xi] The work of Harry Braverman is the classic in this regard. See *Labour and Monopoly Capital* (New York: Monthly Review Press,).

[xii] See e.g. Roy Boyne, Post-Panopticism, *Economy and Society*, 29(2) 2000: 285-307

the Panopticon as an antetype of 'invisible' electronic forms of surveillance, but also of relatively unobtrusive CCTV systems, and those that focus more on the classificatory powers of the Panopticon (an idea that is worked out more fully in relation to Foucault's 'biopower').[xiii] The latter perspective has been explored empirically in several areas, including high-tech policing and commercial database marketing.[xiv] While both aspects of the Panopticon offer some illuminating insights into contemporary surveillance, the latter has particular resonance in the present circumstances. In this view, persons and groups are constantly risk-profiled which in the commercial sphere rates their social contributions and sorts them into consumer categories, and in policing and intelligence systems rates their relative social dangerousness. Responses to September 11 have increased possibilities for 'racial' profiling along 'Arab' lines in particular.

Both the Weberian-Orwellian and the Foucaldian perspectives depend on a fairly centralized understanding of surveillance. However, given the technological capacities for dispersal and decentralization, not to mention globalization, some more recent studies have suggested that a different model is called for. The work of Gilles Deleuze and Felix Guattari[xv] offers some novel directions, suggesting that the growth of surveillance systems is rhizomic; more like a creeping plant than a central tree trunk with spreading branches. This has persuaded some to see surveillance as a looser, more malleable and flowing set of processes – a

---

[xiii] Part of the difficulty is that although the idea of biopower exists in *Discipline and Punish*, it is much more clearly evident in *The History of Sexuality*.

[xiv] Oscar Gandy, *The Panoptic Sort: A Political Economy of Personal Information*, (Boulder CO: Westview, 1993); Richard Ericson and Kevin Haggerty, *Policing the Risk Society*, (Toronto: University of Toronto Press, 1997).

[xv] Gilles Deleuze and Felix Guattari, *A Thousand Plateaus* (Minneapolis: University of Minnesota Press, 1987)

'surveillant assemblage' – rather than as a centrally controlled and coordinated system.[xvi]

In the assemblage, surveillance works by abstracting bodies from places, splitting them into flows to be reassembled as virtual data-doubles, calling in question once again hierarchies and centralized power. One important aspect of this is that the flows of personal and group data percolate through systems that once were much less porous; much more discrete and watertight. Thus, following September 11, surveillance data from a myriad of sources – supermarkets, motels, traffic control points, credit card transaction records and so on – were used to trace the activities of the terrorists in the days and hours before their attacks. The use of searchable databases makes it possible to use commercial records previously unavailable to police and intelligence services and thus draws on all manner of apparently 'innocent' traces.

This brief survey[xvii] of surveillance studies shows how the once-dominant model of centralized state informational power has been challenged by sociol-technical developments. The result is newer models that incorporate the growth of information and communication technologies in personal and population data processing, and more networked modes of social organization with their concomitant flexibility and departmental openness. But is it a mistake to simply leave the other kinds of explanation behind, as we move up (?to the next plateau) using something like Wittgenstein's ladder? Rather than answering this question

[xvi] See e.g. Kevin D. Haggerty and Richard V. Ericson, The surveillant assemblage, *British Journal of Sociology*, 51(4) 2000: 506-622.

[xvii] A longer survey appears in David Lyon, *Surveillance Society: Monitoring Everyday Life*, (Buckingham: Open University Press, 2001).

directly, I shall simply offer a series of questions that once again allow the prism of September 11 aftermath to point up aspects of structure and process that relate in particular to surveillance.

Is surveillance best thought of as centralized power or dispersed assemblage? The responses to September 11 are a stark reminder that for all its changing shape since World War Two the nation-state is still a formidable force, especially when the apparently rhizomic shoots can still be exploited for very specific purposes to tap into the data they carry. Though the Big Brother trope did not in its original incarnation refer to anything outside the nation-state (such as commercial or Internet surveillance that is prevalent today) or guess at the extent to which the 'telescreen' would be massively enhanced by developments first in microelectronics and then in communications and searchable databases, it would be naive to imagine that Big Brother type threats are somehow a thing of the past. Draconian measures are appearing worldwide as country after country instates laws and practices purportedly to counter terrorism. Panic responses perhaps, but they are likely to have long-term and possibly irreversible consequences. The surveillant assemblage can be coopted for conventional purposes.

With regard to the experience of surveillance it is worth asking, is intrusion or exclusion is the key motif? In societies that have undergone processes of steady privatization it is not surprising that surveillance is often viewed in individualistic terms as a potential threat to privacy, an intrusion on an intimate life, an invasion of the sacrosanct home, or as jeopardising anonymity. While all these are understandable responses (and ones that invite their own theoretical responses), none really touches one of the key aspects of contemporary surveillance; 'social

sorting'.[xviii]

The increasingly automated discriminatory mechanisms for risk profiling and social categorizing represent a key means of reproducing and reinforcing social, economic, and cultural divisions in informational societies. They tend to be highly unaccountable – especially in contexts such as CCTV surveillance[xix] – which is why the common promotional refrain, 'if you have nothing to hide, you have nothing to fear' is vacuous. Categorical suspicion[xx] has consequences for anyone, 'innocent' or 'guilty', caught in its gaze, a fact that has poignant implications for the new anti-terror measures enacted after September 11.

The experience of surveillance also raises the question of how far subjects collude with, negotiate, or resist practices that capture and process their personal data? Surveillance is not merely a matter of the gaze of the powerful, any more than it is technologically determined. Data-subjects interact with surveillance systems. As Foucault says, we are 'bearers of our own surveillance' but it must be stressed that this is not merely an unconscious process in which we are dupes. Because surveillance is always ambiguous – there are genuine benefits and plausible rationales as well as palpable disadvantages – the degree of collaboration with surveillance depends on a range of circumstances and attitudes. Under the present

---

[xviii] See David Lyon (ed.) *Surveillance as Social Sorting: Privacy, Risk, and Automated Discrimination*, (London and New York: Routledge, forthcoming)

[xix] Clive Norris and Gary Armstrong, *The Maximum Surveillance Society: CCTV in Britain*, (London: Berg, 1999).

[xx] This elegant concept was first used by Gary T. Marx in *Undercover: Police Surveillance in America* (Berkeley: University of California Press, 1988). I discuss its commercial equivalent, 'categorical seduction' in *The Electronic Eye: The Rise of Surveillance Society*, (Cambridge: Polity Press and Malden MA: Blackwell, 1994).

panic regime (towards the close of 2001) it appears that anxious publics are willing to put up with many more intrusions, interceptions, delays, and questions than was the case before September 11, and this process is amplified by media polarizations of the 'choice' between 'liberty' and 'security'.[xxi] The consequences of this complacency could be far-reaching.

I have mentioned technological aspects of surveillance several times, which points up the question, are these developments technologically or socially driven? To read some accounts – both positive *and* negative -- one would imagine that 'technology' really has the last word in determining surveillance capacities. But this is fact a fine site in which to observe the co-construction of the technical and the social.[xxii] For example, though very powerful searchable databases are in use, and those in intelligence and policing services are being upgraded after September 11, the all-important categories with which they are coded[xxiii] are produced by much more mundane processes. Databases marketers in the USA use crude behavioural categories to describe neighbourhoods, such as 'pools and patios' or 'bohemian mix', and CCTV operators in the UK target disproportionately the 'young, black, male' group. The high-tech glitz seems to eclipse by its dazzle those social factors that are constitutionally imbricated with the technical.

Still on the technical, however, a final question would be, are the proposed new

---

[xxi] I experienced this, anecdotally, when an op-ed piece I wrote under the title 'Whither surveillance after bloody Tuesday?' was published in the newspaper as 'What price in liberty will we pay for security?' *The Kingston Whig-Standard*, September 28, 2001.

[xxii] See David Lyon 'Surveillance technology and surveillance society, in Tom Misa, Philip Brey and Andrew Feenberg (eds.) *Modernity and Technology*, Cambridge MA: MIT Press, forthcoming 2002)

[xxiii] See the influential work by Lawrence Lessig, *Code, and Other Laws of Cyberspace*, (New York: Basic Books, 1999).

anti-terrorist measures pre-emptive or investigatory? Over the past few years an important debate has centred on the apparent switch in time from past-oriented to future-oriented surveillance. Gary T. Marx predicted in the late 1980s[xxiv] that surveillance would become more pre-emptive and in many respects he has been vindicated. This idea has been picked up in a more Baudrillardian vein by William Bogard who argues that surveillance is increasingly simulated, such that seeing-in-advance is its goal.[xxv]

However, this kind of argument easily loses sight of actual data-subjects – persons – whose daily life chances and choices are affected in reality by surveillance.[xxvi] But a parallel assumption, in policy circles, is that new technologies will be able to prevent future terrorist acts. It would be nice to believe this – and as one who was in mid-flight over North America at the time of the attacks I would love to think it true! – but the overwhelming evidence points in the other direction. Surveillance can only anticipate up to a point, and in some very limited circumstances. Searchable databases and international communications interception were fully operational on September 10 to no avail.

Surveillance responses to September 11 are indeed a prism through which aspects of social structure and process may be observed. The prism helps to make visible the already existing vast range of surveillance practices and processes that touch everyday life in so-called informational societies. And it helps to check various

---

[xxiv] See note 20.

[xxv] William Bogard, *The Simulation of Surveillance*, Cambridge and New York: Cambridge University Press, 1996).

[xxvi] See e.g. Stephen Graham, 'Spaces of Surveillant Simulation'

easily made assumptions about surveillance – that it is more dispersed than centralised, that it is more intrusive than exclusionary, that data-subjects are dupes of the system, that it is technically-driven, that it contributes more to prevention than to investigation after the fact.

Sociologically, caution seems to be called for in seeing older, modernist models simply as superseded by newer, postmodern ones. For all its apparent weaknesses in a globalizing world, the nation-state is capable of quickly tightening its grip on internal control, using means that include the very items of commercial surveillance -- phone calls, supermarket visits, and Internet surfing -- that appear 'soft' and scarcely worthy of inclusion as 'surveillance'. And for all the doubts cast on the risk-prone informational, communications, and transport environment, faith in the promise of technology seems undented by the 'failures' of September 11. Lastly, in the current climate it is hard to see how calls for democratic accountability and ethical scrutiny of surveillance systems will be heard as anything but liberal whining. The sociology of surveillance discussed above suggests that this is a serious mistake, with ramifications we may all live to regret.