The architecture of surveillance

Richard Jones writes about the politics and design of surveillance systems and compares the views of leading theorists.

Surveillance studies are today in good health, and raising a questioning voice in the face of what appears to be the roll-out of a never-ending stream of new surveillance technologies. While the 'greats' such as Marx, Weber and Foucault continue to exercise their influence over theoretical approaches, new directions are also apparent. David Lyon's careful sociology continues to inform (see pp 4). Several researchers have revealed the social realities of CCTV system operation and workplace surveillance. Themes of current theoretical interest include the state, identity systems, and the regulation of, as Lyon puts it, the two key areas of 'travel and transaction'; the surveillance of 'mobilities' generally; the nature of 'privacy'; state-commerce relationships; and the politics of surveillance. Here, I will concentrate on just one small issue related to some of these themes, namely how surveillance systems can be designed to emphasise different political values — the theoretical implication of which is that technological system design is more of a political activity than it first appears, and hence bears closer scrutiny.

In his book, *Code*, the American lawyer and Internet theorist Larry Lessig (2006) argues that the internet is regulable not only through law, but also by market forces, social norms, and by what he terms 'architecture'. By this last term, he means the physical or virtual properties of a system, suggesting that in a given system these properties enable and constrain users' behaviour in certain ways. The system design, Lessig argues, typically expresses or supports certain political values. For example, a computer network could be designed to protect users' anonymity, or alternatively it could be designed to permit easy identification of users by others. Elsewhere, I have argued that Lessig's model has interesting parallels with the more clearly criminological work of Anthony Bottoms on compliance; and with R.V. Clarke and colleagues' development of situational crime prevention typologies. I have also shown how a model synthesised from these approaches can be applied to fields as disparate as cybercrime, punishment, and policing (see, for example, Jones 2007). Much of this work focuses on physical or virtual constraints. Can the notion of 'architecture' also be applied to the study of surveillance systems, seemingly designed more to watch rather than constrain—and if so, what if anything does this tell us?

In fact, architecture accounts not just for what users can and can't do within a given system, but also for what administrators can and can't know or do about those users. (I use the term 'administrators' to refer to anyone from a CCTV scheme operator, through to state security services; and 'users' to refer to the end users of physical or virtual spaces.) In other words, the term 'architecture' relates to the overall operating properties of a given system. These properties typically cast a (political) relation between users and administrators, and different technological designs can support different political values. An online discussion board system might for example be designed to promote user anonymity ('privacy') or instead be designed to enable identification of discussants ('security').

There are a number of dimensions to surveillance architecture that are of interest from a privacy perspective. One is whether the system design enables users to tell whether they're being monitored or not: the visibility or invisibility of the surveillance system. (Perhaps this is a spectrum, running from the overt surveillance of visible observation by a police officer, for example; through what Michel Foucault termed the 'visible and unverifiable' surveillance of the Panopticon (or, today, an unconcealed CCTV camera: you can see it's there, but can't tell if you're being watched); to covert surveillance.) A second is whether the technology simply 'monitors' activity as it happens, or whether it additionally or instead stores a 'searchable' record (Lessig, 2006: 202). One of the privacy challenges of 'digital surveillance' lies in the capabilities enabled by database search. A third (and related) dimension, and perhaps the most obvious, is the degree to which the surveillance system design protects or intrudes upon users' anonymity. Rotenberg (2001), following others, distinguishes between 'Privacy Enhancing Technologies' (PETs) and 'Privacy Intrusive Technologies' (PITs). PETs can include '[e]ncryption, anonymous web-browsing, filtering devices... privacy-preference tools and the like', and can offer some degree of privacy, though they are no panacea (Ball et al., 2006: 83-84). The point to note here, however, is simply that not all surveillance is similarly intrusive.

Lessig coins the term 'digital surveillance' to describe a 'very specific kind of surveillance', in 'which some form of human activity is analysed by a computer according to some specified rule'

Continued on next page

(Lessig 2006: 209; see also Graham and Wood 2003), an area that David Lyon and others have explored in detail (see for example Lyon 2002). A challenge for 'friends of privacy' in respect of digital surveillance is to establish what exactly it is about discrete, automated, computerised surveillance that remains objectionable. Lessig suggests three possibilities: such searches offend a person's dignity; they are intrusive; or they represent insufficient limits on government power over individuals.

In some respects Lessig's work echoes Packer's earlier account of two opposing models of the criminal process. Indeed, in his famous book *The Limits of the Criminal Sanction*, Herbert Packer (1969) discusses the electronic surveillance of the time in the context of considering competing 'Due Process' and 'Crime Control' ideologies during the initial phases of the criminal process. Although written before the emergence of 'digital surveillance' technologies, and focusing on the then 'war on organised crime' (which today we might transpose to the 'war on terror'), arguably many of the basic issues relating to surveillance remain the same. Packer recognises that surveillance technologies 'pose increasingly difficult problems for the criminal process as pressure from law enforcement for license to enlist these devices in the investigation of crime meets counterpressure from people who see the doom of individual freedom in a wholesale intrusion by government into the private lives of its citizens' (1969: 195).

In the case of electronic surveillance, the 'Crime Control Model' expresses strong support for its use by law enforcement officials, maintaining that while abuses may sometimes occur this is a price worth paying, and that in general, 'Law-abiding citizens have nothing to fear' (1969: 195-196). The 'Due Process Model' on the other hand, argues that 'The right of privacy... cannot be forced to give way to the asserted exigencies of law enforcement'. Moreover, knowledge of unchecked surveillance 'would certainly inhibit the free expression of thoughts and feelings that makes life in our society worth living' (1969: 196-197).

A distinctive feature of Packer's book was his role-play of the two competing positions, on the issues at each stage of the criminal process, showing how the respective positions taken express not merely the prioritising of due process over crime control goals (or vice versa), but also express a wider political ideological stance, turning ultimately on the relationship between individual and state. Introducing Packer's model into the surveillance and privacy debates is helpful then, I think, because it helps us locate these debates within a still deeper political antagonism, namely between Due Process and Crime Control values. From this perspective, privacy concerns surrounding surveillance become more clearly related to debates elsewhere in criminal justice, such as about prisoners' human rights. Indeed ultimately Packer's thesis is about competing political views on law, and specifically about legal protections afforded to individuals as against the state. Lastly, Packer's model is useful in suggesting a framework characterising the ideologies expressed in the designs of intrusive surveillance technologies (such as 'backscatter' x-ray body scanners) and in the pro-privacy objections to such technologies.

In conclusion, my argument here is that Lessig's and Packer's models are useful in helping us distinguish between surveillance systems in terms of the political values embedded therein. Of course, this is not the end of the matter, and how the system operators actually use the systems clearly remains of crucial importance. However, system design is likely to influence system use at some level, and further exploration of the properties, features and uses of surveillance systems may help us cast further light on this still often hidden area.

■

Dr Richard Jones *is based at Edinburgh Law School, University of Edinburgh.*

References

Ball, K. *et al.* (2006) *A Report on the Surveillance Society*. Surveillance Studies Network.

Graham, S. and Wood, D. (2003) 'Digitizing surveillance', *Critical Social Policy*. Vol. 23(2): 227-248.

Jones, R. (2007) 'The Architecture of Policing' in A. Henry and D.J. Smith (eds) *Transformations of Policing*. Aldershot: Ashgate.

Lessig, L. (2006) *Code version 2.0*. New York: Basic Books.

Lyon, D. (2002), *Surveillance as Social Sorting*. London: Routledge.

Packer, H. (1969) *The Limits of the Criminal Sanction*. London: OUP

Rotenberg, M. (2001) 'Fair Information Practices and the Architecture of Privacy', *Stanford Technology Law Review 1*.