David Lyon

The End of Privacy?

From the late twentieth century a common response to the massive growth of surveillance systems in the global north has been to ask whether we are witnessing the "end of privacy". What is meant by this? On the one hand, as many socially critical authors assert, there are fewer and fewer "places to hide" (see, e.g. O'Harrow 2005) in the sense that some surveillance systems record, monitor or trace so many of our daily activities and behaviours that, it seems, nothing we do is exempt from observation. On the other, a different set of authors see the "end of privacy" as something to celebrate, or at least not to lament. In the face of growing e-commerce and the consequent mass of personal data circulating, Scott McNealy, of Sun Microsystems, most famously declared, "Privacy is dead. Get over it!"

It is important to note that privacy is a highly mutable concept, both historically and culturally relative. If privacy is dead, then it is a form of privacy—legal, relating to personal property, and particularly to the person as property—that is a relatively recent historical invention in the western world. At the same time, this western notion of privacy is simply not encountered in some South-East Asian and East countries. The Chinese have little sense of personal space as westerners understand it, and the Japanese have no word for privacy in their language (the one they use is imported from the west).

The best-known writer on privacy in a computer era is Alan Westin, whose classic book, *Privacy and Freedom* (Westin 1967) has inspired and informed numerous analysts and policy makers around the world. For him, privacy means that "... individuals, groups or institutions have the right to control, edit, manage and delete information about themselves and to decide when, how and to what extent that information is communicated to others." However, although this definition seems to refer to more than the "individual," the onus of responsibility to "do something" about the inappropriate use of personal (and other) data is on data-subjects. That is, rather than focussing on the responsibilities of those who collect data in the first place, it is those who may have grievances who have rights to have those addressed.

This emphasis has been questioned, for example by Priscilla Regan (1995) who argues that privacy has intrinsic common, public and social value, and that that therefore not only may individuals have a right to seek protection from the effects of misused personal data, but also organizations that use such data have to give account. The huge increase in surveillance technologies, for instance in the workplace and in policing, underscores this point. Today, data are not only collected and retrieved, but analysed, searched, mined, recombined and traded, within and between organizations, in ways that make simple notions of privacy plain inadequate. Valerie Steeves maintains that while Westin started out (in the 1960s) with a broader definition of privacy, the overwhelmingly individualistic context of American business and government interests, in conjunction with pressure to adopt new technology "solutions" has served to pare down privacy to its present narrow conception (Steeves 2005).

Surveillance as social sorting

To argue that privacy may not have the power to confront contemporary surveillance in all its manifestations is one thing. To propose an alternative approach is another. For, as in the case of the Orwellian and the panoptic imagery for capturing what surveillance is about, the language of privacy has popular cachet. It is difficult to explain why "privacy" is not the (only) problem that surveillance poses (Stalder 2002) when this is so widely assumed by lawyers, politicians, mass media and western publics. The best way of deflecting attention from a singular focus on privacy, in my view, is to consider surveillance as "social sorting."

One might say that "to classify is human" but in modern times classification became a major industry. From medicine to the military, classification is crucial. As Geoffery Bowker and Susan Star show, the quest for meaningful content produces a desire for classification, or "sorting things out" (Bowker and Star 1999). Human judgements attend all classifications and, from our perspective, these are critical. Classification allows one to segregate undesirable elements (such as those susceptible to certain kinds of disease) but it is easy for this to spill over into negatively discriminatory behaviours. South Africa under apartheid had a strong population classification system but it served to exclude, on "racial" criteria, black people from any meaningful access to opportunity structures. Classification may be innocent and humanly beneficial but it can also be the basis of injustice and inequity. The modern urge to classify found its ideal instrument in the computer.

One way of thinking about surveillance as social sorting is to recall that today's surveillance relies heavily on ICTs. Both security measures and marketing techniques exploit the interactivity of ICTs to identify and isolate groups and individuals of interest to the organizations concerned. By gathering data about people and their activities and movements and analysing secondary data (by "mining" other databases) obtained through networked technologies, marketers can plan and target their advertising and soliciting campaigns with increasingly great accuracy. Equally, security personnel use similar strategies to surveil "suspects" who have been previously identified or who fit a particular profile in the hope of building a fuller picture of such persons, keeping tabs on their movements, and forestalling acts of violence or terror.

These actuarial plans for opportunity maximization (marketing strategies for widening the range of target groups for products and services) and for risk management (such as security strategies for widening the net of suspect populations) represent a new development in surveillance. Though they have a long history, they contrast with more conventional reactive methods of marketing or security delivery. They are future rather than past oriented, and are based on simulating and modelling situations that have yet to occur. They cannot operate without networked, searchable databases and their newness may be seen in the fact that unsuspecting persons who fit, say, an age profile, may be sent email messages promoting devices guaranteeing enhanced sexual performance and others, much less amusingly, who simply fit an ethnic or religious profile, may be watched, detained without explanation or worse by security forces.

The "surveillant assemblage" works by social sorting. Abstract data of all kinds—video images, text files, biometric measures, genetic information and so on—are manipulated to produce profiles and risk categories within a fluid network. Planning, prediction, pre-emption, permitting, all these and more goals are in mind as the assemblage is accessed and drawn upon. Social sorting is in a sense an ancient and perhaps inevitable human activity but today it has become routine, systematic and above all technically assisted or automated (and in some sense driven). The more new technologies are implicated, however, the more the criteria of sorting become opaque to the public. Who knows by what standards a credit was unexpectedly turned down or an innocent terrorist suspect was apprehended? Of course, the sorting may be innocent and above question—surveillance, after all, is always ambiguous—but it is also the case that social sorting has a direct effect, for good or ill, on life-chances (see Lace 2005:28–32 for consumer examples). The main fears associated with automated social sorting, then, are that through relatively unaccountable means, large organizations make judgments that directly affect the lives of those whose data are processed by them. In the commercial sphere, such decisions are made in an actuarial fashion, based on calculations of risk, of which insurance assessments provide the best examples. Thus people may find themselves classified according to residential and socio-demographic criteria and paying premiums that bear little relation to other salient factors. Equally, customers are increasingly sorted into categories of worth to the corporation, according to which they can obtain benefits or are effectively excluded from participation in the marketplace. In law enforcement contexts, the actuarial approach is replicated; indeed, Feely and Simon warned in the mid 1990s that forms of "actuarial justice" were becoming evident. The "new penology", they argue, "is concerned with techniques for identifying, managing and classifying groups sorted by levels of dangerousness" (Feely and Simon 1994: 180). Rather than using evidence of criminal behaviour, newer approaches intervene on the basis of risk assessment, a trend that has become even more marked after 9/11.

Surveillance society and safety state

The growth of the surveillance dimension of modern states warrants special attention and one way of indicating this is to refer to current conditions of social life as living in a "surveillance society". This is no more meant to be sinister than it is to refer to everyday practices of extracting personal data in the supermarket—for example—as "surveillance." It simply draws attention to a key feature of contemporary life which is both so routine and taken-for-granted that it seems unremarkable and yet simultaneously has such far-reaching consequences that it demands social scientific scrutiny.

At the same time, life in a surveillance society reflects in part some expanding dimensions of the nation-state. Whereas in the mid and later twentieth century it may have been true to say that several more liberal countries considered themselves to be "welfare states", in the early twentieth century the designation "safety state" began to be more plausible as an overall descriptor (Raab 2005). More and more, the criteria by which policies of many kinds are judged is not the positive benefit for all so much as the minimization of risk. New technologies designed to reduce risk are central to the emerging quest for the "safety state", and they all entail surveillance of one kind or another.

In their work on policing, Ericson and Haggerty show how new communication technologies make possible faster transmission and contribute to a shift from local spatial emphases to "microcentres of inscription" such as computer terminals in police cars (1997: 431). Organizational hierarchies are challenged by the same trends, and at the same time more "remote control" becomes possible. In combination, the new technologies enable faster surveillance of the population for risk management purposes (as well as making the police themselves more vulnerable to scrutiny). What they say about policing has a familiar ring in other sectors as well. Surveillance is vital to risk communication because it "provides knowledge for the selection of thresholds that define acceptable risks and justify inclusion and exclusion." Thus, they go on, "coercive control gives way to contingent categorization" and everyone is "assumed to be 'guilty' until the risk communication system reveals otherwise ..." (1997: 449).

Such trends have become more widespread and controversial in the West since 9/11. Airport and border management systems are on heightened alert according to just the same kind of criteria. The same kinds of surveillance systems, now further bolstered by the adoption of "new" biometrics technologies (distinguished from the "old" not because they have transcended their often racist and colonial "anthropometric" origins but rather by their extensive use of ICTs), are used for making "biographical" profiles of human populations to determine whether or not they may travel, exchange large sums of money, or be employed within given companies. Hence the scandals, from a civil liberties perspective, of "no-fly lists" based on ethnicity, religion, or country of origin, that can also easily include "mistaken identities." Hence too, the ironic exacerbation of risk (to travellers and citizens) from the increasing reliance on other agencies (such as airport) to whom tasks have been outsourced, especially in countries such as the USA.

It is also, at least in part, the role played by ICTs that makes it important to consider both "surveillance society" and "safety state" together. For the kinds of risk communication (that may also be read as"opportunity calculation') carried out by firms in relation to customers, and providing detailed profiles, are also of interest to the nation state. Not only are the methods of assembling profiles based on similar algorithms, the actual data gathered and analysed by those firms is also of interest to law enforcement agencies, especially in the so-called "war on terrorism." Thus in 2006, for instance, Google refused to hand over its search records to the US Department of Justice (DoJ), citing the privacy of its users and the protection of its trade secrets. In this particular case, the DoJ claimed they wished to test the effectiveness of web-filtering software but many civil libertarians and privacy advocates saw it as the thin end of the wedge. Government could also use search records to obtain highly personal records, in the name of "national security."

Thus while it is worth examining both the development of the "surveillance society" for its routine dependence on the garnering and processing of personal data, and the"safety state" for its use of surveillance for risk communication, it is also important to see that the two work in an increasingly symbiotic relation with each other. If present trends continue, this particular social-economic-political nexus will become more and more significant in coming decades.

Politics of personal data

Surveillance studies, as this sub-field is increasingly known (see Lyon, forthcoming), has often focused on the large-scale systems, institutions and technologies that promote and produce surveillance. This can result in some rather negative and dystopian perspectives, however, that give the impression that ordinary people whose everyday activities are surveilled are simply pawns, ciphers in an increasingly global surveillance machine. Without suggesting that such views have no merit, or that the balance of power is not tipped overwhelmingly in favour of those large institutions, it is nevertheless important to note that surveillance is an interactive process. What sociologists of technology call "co-construction" describes well the world of surveillance (Lyon, 2004).

In order to work, surveillance systems depend on their subjects (indeed, as Foucault observed a long time ago, subjects become "the bearers of their own surveillance" 1979). Although there is a sense in which the subjects of surveillance become"objectified' as their data doubles become more real to the surveillance system than the bodies and daily lives from which the data have been drawn, their involvement with surveillance systems often remains active, conscious and intentional. People comply (but not as dupes), negotiate and at times resist the surveillance systems in which their lives are enmeshed.

It is very important to consider the ways in which so-called "data subjects" of contemporary surveillance engage with and respond to having their data collected and used by organizations. Much depends on the purposes for which those data are collected. Righteous indignation at being shut out of a flight may be the response of a passenger with a "suspicious" name, even though that same passenger may be delighted with the "rewards" from his frequent flyer program with which he "bought" the ticket. In each case, extensive personal data is used to determine the outcome, whether the privileged category of an "elite" passenger or the excluded category of a name on the no-fly list. Consumers appear most willing to provide their personal data, in the belief that some benefit awaits them; employees and citizens are much more likely to exercise caution or express complaint at the over-zealous quest of organizations for their details.

Other variables in the analysis of the interactions between the "watchers and the watched" include the extent of "data subjects'" knowledge of being watched. In the classic case of panoptic surveillance, prison inmates were supposed to subject themselves to self-discipline based on the assumption that the unseen inspector might just be watching. The uncertainty is essential to the success of the system. But what of situations where cameras are hidden, or when customer details are simply extracted without the knowledge of the person concerned? Life-chances and choices are still affected, for better or for worse, but the opportunity to engage with the surveillance system is severely restricted. As ICTs help to reduce the visibility of surveillance through miniaturization or automation, this will become an increasingly significant area for social and political analysis.

The evidence suggests that the politics of information is becoming more important, even though some leading theorists of information may miss it. Manuel Castells, for instance, reassures his readers that for most of the time contemporary surveillance is a rather benign set of processes and Scott Lash argues that with the"predominance of communication the logic of classification disappears" (2002: 112). Yet as I have tried to show here, the use of ICTs within new regimes of risk management in the surveillance society and the safety state is contributing to new modes of classification that have profound social, economic and political ramifications. This is where the struggle over information will take place.

This is an extract reprinted from David Lyon's chapter in *The Oxford Handbook of Information and Communication Technologies,* edited by Robin Mansell, Chrisanthi Avgerou, Danny Quah, and Roger Silverstone, © Oxford University Press, 2007. For further information, please see *http://www.oup.com/uk/catalogue/?ci=9780199266234*.

O'Harrow R. (2005), *No Place to Hide,* New York: Free Press.
Westin, A. (1967), *Privacy and Freedom,* New York: Athenaeum.
Steeves, V. 2005 "It's not child's play: The online invasion of children's privacy," *University of Ottawa Law and Technology Journal,* 2 (2).
Stalder, F. (2002), "Privacy is not the antidote to surveillance", *Surveillance and Society* 1(1),
Bowker, G. and Star, Susan. (1999), *Sorting things out: Classification and its consequences,* Cambridge MA: MIT Press.
Lace, S. (2005) *The Glass Consumer: Life in a Surveillance Society,* Bristol UK: The Policy Press
Feely M.and Simon, J. (1994) "Actuarial justice: the emerging new criminal law" in D.Nelken ed. *The Futures of Criminology,* London: Sage.
Raab, C. D. (2005), "Governing the safety state", inaugural lecture at the University of Edinburgh, Scotland (June 7).
Ericson, R. and Haggerty, K. (1997), *Policing the Risk Society,* Toronto: University of Toronto Press.
Lyon, D. (2004), "Surveillance technologies and surveillance societies", in T. Misa, P. Brey, and A. Feenberg, (eds.) *Modernity and Technology,* Cambridge MA: MIT Press.