6

Opposing surveillance

Brian Martin

Professor, School of Social Sciences, Media and Communication,
University of Wollongong

Abstract

If surveillance is potentially seen as unfair, then it is predictable that its proponents will use a number of methods to reduce public concern: cover up surveillance activities, devalue targets and opponents, offer plausible interpretations for actions, use official processes that give an appearance of fairness, and intimidate and bribe targets and opponents. Opponents of surveillance can be more effective by being prepared for these tactics and working out ways to counter them.

Keywords: surveillance, tactics, opposition, outrage, resistance

1 Introduction

Over the years, many people have opposed surveillance, seeing it as an invasion of privacy or a tool of social control. Dedicated campaigners and concerned citizens have opposed bugging of phones, identity cards, security cameras, database linking and many other types of surveillance. They have lobbied and campaigned against abuses and for legal or procedural restrictions. Others have developed ways of getting around surveillance.

In parallel with resistance, there have been many excellent critiques of surveillance, exposing its harmful impacts and its role in authoritarian control (e.g., Dandeker 1990; Gandy 1993; Garfinkel 2000; Holtzman 2006; Lyon 1994, 2003; Marx 1988; Murray 1993; Rosen 2000). However, comparatively little is written about tactics and strategy against surveillance. Indeed, social scientists have little to say about tactics and strategy in any field (Jasper 2006: xii-xiii). My aim here is to present a framework for understanding tactics used in struggles over surveillance.

Actions that are seen to be unfair or to violate social norms can generate outrage among observers (Moore 1978). Nonviolence researcher Gene Sharp (1973: 657-703) found that violent attacks on peaceful protesters — something that many people see as unjust — could be counterproductive for the attackers, generating greater support for the protesters among the protesters' supporters, third parties and even the attacking group. Because of this potential for attacks to be counterproductive, attackers, by design or intuition, may take steps to reduce possible outrage. By examining a wide range of issues — censorship, unfair dismissal, violent attacks on peaceful protesters, torture and aggressive war — a predictable pattern in tactics can be discerned: perpetrators regularly use five sorts of methods to minimise adverse reactions to their actions (Martin 2007).

1. Cover-up: the action is hidden or disguised.
2. Devaluation: the target of the action is denigrated.
3. Reinterpretation: plausible explanations are given for the action.
4. Official channels: experts, formal investigations or courts are used to give an appearance of justice.
5. Intimidation and bribery: targets and their allies are threatened or attacked, or given incentives to cooperate.

This is called the backfire model: when these methods are insufficient to dampen public outrage, the action can backfire on the perpetrator. However, backfire is rare: in most cases, the methods work sufficiently well to minimise outrage.

Consider an example different from surveillance: police use force in arresting someone. This has the potential to cause public outrage if the force used is seen as unnecessary, excessive or vindictive. Police in these circumstances regularly use one or more of the five methods. If possible, they undertake the arrest out of the public eye. They refer to the person arrested as a criminal or by derogatory terms. If challenged, they claim arrestees were resisting and that using force was necessary and carried out according to protocol. They refer those with grievances to official complaints procedures, which almost always rule in favour of the police. And they may threaten the arrestee with criminal charges should they make a complaint (Ogletree et al. 1995).

On 3 March 1991, Los Angeles police arrested a man named Rodney King, in the course of which King was hit by two 50,000-volt tasers and beaten with metal batons more than 50 times. This arrest would have gone unnoticed except that George Holliday, who lived nearby, recorded the beating on his new videocamera. When footage was shown on television, it caused a massive public and political reaction against the Los Angeles police. Holliday's videotape cut through the normal cover-up and allowed viewers to judge the events for themselves, overriding the police's interpretation of the events and the media's normal police-sympathetic framing (Lawrence 2000). Nevertheless, in the ensuing saga the police and their supporters used every one of the five methods of inhibiting outrage — though, unusually, in this case their efforts were unsuccessful in preventing a huge backlash against the police (Martin 2005).

Tactics for and against surveillance can be analysed using the same framework. The foundation for public outrage is a sense of unfairness. This is certainly present at least some of the time: people may see surveillance as an invasion of privacy (as with hidden video cameras), as a tool of repression (as in monitoring dissenters) or a tool of exploitation (as in monitoring of workers). The very word "surveillance" is a tool in opposing it, because the word has such negative connotations.

A sense of unfairness is not inherent in the act of observing someone or collecting and analysing data about them. People's sense of unfairness is the subject of a continual struggle, with privacy campaigners trying to increase concern and purveyors of surveillance techniques trying to reduce it. Methods to inhibit or amplify outrage are used within the prevailing set of attitudes and in turn affect those attitudes.

Given that some people see surveillance as inappropriate, unfair, dangerous or damaging, there is a potential for resistance and hence it is predictable that one or more of the five methods of inhibiting outrage will be deployed. In the remainder of this paper, I look at each of the five methods of inhibiting outrage and ways to challenge these methods.

The five-method classification used here is a convenient framework for examining tactics for and against surveillance. To use this framework does not require actors to be consciously engaging in a struggle, as many are simply reacting to the circumstances in which they find themselves. For those who are concerned about surveillance, though, it is useful to think in terms of tactics and strategies.

2 Cover-up and exposure

Surveillance is commonly carried out in secret. When people don't realise it's happening, they are far less likely to become concerned about it. The secrecy covering surveillance is part of a wider pattern of government and corporate secrecy (Roberts 2006).

Political surveillance of individuals is normally done surreptitiously. Bugs are installed in residences; telephones are tapped; remote cameras record movement; police in plain clothes observe at a discrete distance. There is an obvious reason for this: targets, if they know about surveillance, are better able to avoid or resist it. But secrecy is maintained beyond operational necessities: in most cases, the existence of surveillance is kept secret long afterwards, often never to be revealed. Exposures may require exceptional circumstances (Marx 1984), such as the collapse of East Germany's communist regime or the "liberation" of FBI files at Media, Pennsylvania in 1971 by the Citizens' Commission to Investigate the FBI (Cowan et al. 1974). When surveillance is exposed, for example FBI surveillance of individuals such as Martin Luther King, Jr. and John Lennon, it can cause outrage. The revelation that the National Security Agency had been spying on US citizens since 2002 caused a massive adverse reaction.

Employers sometimes do not want to tell workers they are being monitored, when there is a possibility this may stimulate individual or collective resistance. (On other occasions employers are open about monitoring, when this serves to induce compliance.)

Under the US Patriot Act, the FBI can obtain secret warrants to obtain records from libraries, Internet service providers and other organisations. The organisations subject to this intrusion cannot reveal it, under severe penalties. This draconian enforcement of secrecy serves to reduce personal and popular concern about surveillance, for example when the Patriot Act is used against non-terrorist groups such as antiwar protesters.

In some cases, surveillance becomes routinised, so cover-up is less important. In many areas, camera monitoring is carried out openly: it is possible to observe oneself, on a screen, walking into a shop. On the other hand, some forms of surveillance are hidden so effectively that they are completely outside of most people's awareness, for example collection of web data, meshing of database files, police checks on car licence numbers and recording of bank transactions.

The importance of low visibility in enabling surveillance to continue and expand is apparent through a thought experiment: imagine that you received, at the end of every month, a list of instances in which data had been collected about you, by whom and for what purpose. Imagine knowing whether you had been placed on a list to be denied a loan or a job.

Exposing surveillance is crucial to challenging it. Exposure requires collection of information, putting it into a coherent, persuasive form, providing credible backing for the evidence, and communicating to a receptive audience. Sometimes a single person can do all of these steps, collecting information directly and publishing it on the web. Normally, though, a chain of participants is involved, for example an insider who leaks documents, a researcher who prepares an analysis, a journalist who writes a story and an editor or producer who publishes it. Campaigners help in exposure, as with Privacy International's Big Brother Awards for organisations with bad records in threatening privacy.

3 Devaluation and validation

If a person is perceived as unworthy, then people don't get as upset when bad things are done to them. Executing an innocent person is seen as outrageous; executing a serial murderer elicits less concern. The inmates of the US prison at Guantánamo were portrayed as the "worst of the worst"; abrogating the civil rights of people painted as terrorists was accepted by much of the population, at least initially.

It is to be expected, therefore, that proponents of surveillance will denigrate targets as a means to justify their operations. Three popular labels for targets of surveillance are criminals, terrorists and paedophiles. Who could be opposed to fingerprinting welfare recipients if it prevents cheating? Who could be opposed to monitoring of emails or cameras on every street corner if it helps deter paedophiles? Furthermore, devaluation is extended to those who oppose surveillance, who are said to be defending criminals, terrorists and paedophiles.

The trite expression "If you have nothing to hide, you have nothing to fear" is built on an implicit devaluation: if you're concerned about privacy and surveillance, you must have something to hide, which implies you're guilty and devious (Marx 2007). Therefore, surveillance seems to be justified.

One way to challenge devaluation is to emphasise the essential humanity of every individual. A powerful way to do this is to make targets human, by using names, photos and personal details. Australian David Hicks was incarcerated without trial at Guantánamo for over five years without trial, and stigmatised by the Australian government as a terrorist. Opponents of Hicks' treatment were eventually able to generate concern, using photos of Hicks to make him appear as an ordinary person. Hicks' father Terry spoke out on his behalf, as did his US military lawyer Michael Mori: having valued allies helps counter devaluation.

The same principle applies to validating targets of surveillance. Personal stories of individuals subject to political surveillance are potent tools for validation. For example, Penn Kimball (1984) in his book *The File* poignantly tells of discovering spy agency files about himself in 1978, three decades after they were initiated on a flimsy pretext. The 2006 German film *The Lives of Others* encouraged the viewer to identify with the targets of East German political surveillance and with the Stasi agent who came to sympathise with them. Personal stories of innocent victims of surveillance gone wrong are similarly powerful. A few people will respond to abstract arguments about human rights; many more will respond to personal stories. George Orwell's novel *1984,* a powerful portrait of a dystopian future, uses the personal story of Winston Smith to make larger political points.

4 Interpretation struggles

Proponents of measures that increase surveillance typically provide a justification, often in terms that resonate with widely accepted values. Identification of vehicles is to monitor traffic, detect lawbreakers or collect congestion fees; compilation of corporate databases is to increase efficiency and provide better customer service; cameras are to prevent crime; identity cards are to reduce fraud; baggage checks are to prevent terrorism. The most effective justifications have an element of truth, sometimes quite a large element. The increase in surveillance is simply a by-product, deemed insignificant and unproblematical.

Proponents typically exaggerate the effectiveness of measures. One powerful way to do this is to treat effectiveness as self-evident. Cameras on public streets deter crime, of course. Who could doubt it? Seldom is empirical evidence provided; perhaps little is collected or sought. This is an especially potent technique because it doesn't require the public to trust what authorities say, because members of the public are the ones drawing the conclusion. Airline travellers who, in order to fly, tolerate pointless checks through bags and removal of fingernail files and nail clippers may not question the assumption that such measures are deterring terrorists.

Proponents seldom discuss alternative ways of accomplishing the same goal. An alternative approach to aircraft hijackings is to train passengers in how to communicate with each other and organise to overcome terrorists, as occurred spontaneously on 9/11 United Airlines flight 93 (Scarry 2003). This approach involves trusting passengers and increasing their awareness and skills rather than treating them as potential terrorists. It is seldom mentioned by government authorities, who focus exclusively on measures that give agencies greater power. Radical alternatives are seldom articulated. Rather than keep extensive records on poor people to prevent them cheating on welfare, an alternative is to increase the level of free distribution. For example, free or low-cost food could be provided to anyone who wants it, an expansion of current welfare services. This would reduce the need to monitor individuals.

Problems with surveillance systems are typically said to be rare or non-existent. Sometimes, though, surveillance abuses are publicised, for example cases in which someone has been denied a loan due to incorrect information on a database. These are explained away as rare mistakes. Then there are the systemic abuses, such as the illegal selling of information from databases — for example those held by police — to private investigators and others. These are commonly attributed to rogue operators. The system of information collection is not blamed.

In summary, proponents of surveillance typically provide a plausible justification for measures, exaggerate or simply assume their effectiveness, ignore alternatives and explain away abuses as rare events due to rogue elements.

Opponents of surveillance have challenged every one of these interpretative techniques. Most importantly, they have highlighted the potential of existing or potential systems to increase unnecessary and damaging surveillance. They have challenged claims or assumptions about effectiveness. They have proposed alternatives. And they have argued that abuses are symptoms of flawed systems.

One of the key elements of interpretation struggles is the language used. Proponents of intrusive measures almost never use the word "surveillance." For example, cameras are called security cameras, not surveillance cameras. What about opponents? It is common to refer to use the language of "privacy," which resonates with people's concerns about the sanctity of private life. But privacy rhetoric has disadvantages, in particular that it is personal in focus, whereas surveillance is largely an institutional practice (Stalder 2002).

John Gilliom (1994) analysed the arguments used for and against compulsory drug testing in US workplaces in the 1980s. Proponents justified testing mainly in terms of safety at work, the drug problem generally and the productivity of drug users, whereas opponents mainly cited privacy followed by legal rights, testing error and other concerns, of which surveillance was mentioned by only a few. Gilliom argues that rights discourse was limited because the law is constructed to serve the powerful, and improvements in drug test methods addressed concerns about errors while allowing the testing to continue. The implication of Gilliom's analysis is that opponents' choices of arguments against testing can have a major influence on the success of opposition generally, because arguments lead to particular ways of challenging testing — including legal methods, a form of official channel.

5 Official channels

Courts, ombudsmen, grievance procedures and formal inquiries are examples of official channels. Many people believe that these provide justice. They do in quite a few cases, but when the perpetrator is far more powerful than the victim, official channels typically give only an illusion of justice. For example, some people who speak out in the public interest are nominally protected by whistleblower laws, but in practice these laws provide little or no protection (De Maria 1999). Official channels are typically slow, focused on procedural technicalities, dependent on experts (such as lawyers) and keep matters out of the public eye. They are the exact opposite of using publicity to mobilise public concern. Regulatory agencies for protecting privacy fit this mould.

Some opponents of drug testing in US workplaces took cases to courts, some of which opposed testing. However, the Supreme Court supported testing, so the legal approach failed overall (Gilliom 1994). Along the way, it soaked up a large amount of money and effort, took a long time, distracted energy away from other opposition options, and enabled proponents to achieve an authoritative legal opinion in favour of testing.

In Australia, the Privacy Commissioner, a government-funded office, can receive complaints and make judgements. But its role is severely constrained. The Commissioner has to operate within the current law, which for example does not cover private sector uses of information. As soon as the law is changed, for example to allow another type of database matching, the Commissioner must accept this as the new framework for judging privacy concerns. Furthermore, the Commissioner cannot do much to oppose any practices that it judges to be violations. Anyone who looks to the Privacy Commissioner for relief from actual invasions of privacy, or to halt a new practice, is likely to be disappointed (Davies, 1996).

In most countries, government agencies charged with protecting privacy have been ceding ground for decades. There are some legislative and administrative constraints on surveillance, to be sure, but agencies provide little for anyone seeking redress. If you know or suspect that your employer has been monitoring your email, that your telephone company has been releasing logs about your calls or that information about your purchases is on a corporate database, you can approach any number of agencies, most likely to find out that either the practice is legal, that you have no right to know, or that no information is available to you.

There are many people working in or with agencies who are dedicated to the public interest. The problem is not motivation but the role of agencies in the social structure: they are given limited mandates and inadequate funding, must operate according to bureaucratic regulations and have little or no capacity to initiate significant change. They can be simply overwhelmed by contrary forces, such as the post-9/11 war on terror. Finally, a really effective agency, that gets in the way of powerful interests, is likely to have its funding cut or mandate restricted.

The implication is that opponents of surveillance should not look to official channels as the solution. Stronger laws and well-funded oversight bodies can be worthwhile, but it is a mistake to put too much energy into promoting them, especially because reforms can so easily be rolled back (Olmsted 1996). Increasing public concern should be the primary goal, and that means publicising the issues, gaining supporters, building alliances and developing campaigns. If these efforts are effective, it is likely that governments will create or bolster official bodies to try to convince people that the problem is well in hand.

In 2005, the British government introduced the Serious Organised Crime and Police Act, which includes a provision requiring protesters within one kilometre of Parliament Square to obtain a permit, a requirement that allows files on radicals to be compiled. To even wear a T-shirt with a slogan requires a permit. Activist comedian Mark Thomas (2007) promoted "Mass Lone Demos" by thousands of people with diverse causes, for example some opposing the Iraq war and others whimsically opposing the month of February, overloading the police with permit requests and making fun of the law.

6 Intimidation, bribery and resistance

Surveillance measures can be intimidating: no one likes to imagine that their conversations and actions are being recorded. Having one's photo and fingerprints taken by a government body can be humiliating and stigmatising. Intimidation serves to reduce expressions of resistance. Local critics of surveillance abuses are likely to come under increased surveillance themselves, rather like the way peace activists can end up on US government no-fly lists. (Prominent critics may be a bit safer, because surveillance of them, if discovered and disclosed, could generate more publicity).

There is also a parallel process of encouragement to go along with intrusive measures. If you supply your identification card, you have access to government services. If you allow cookies, you have access to certain websites. If you allow your licence number to be recorded, you can drive on certain roads. Surveillance often comes along with benefits. Accepting the benefits creates a psychological debt: a greater willingness to accept surveillance.

To oppose surveillance, there need to be some people willing to resist. Insiders, with knowledge of abuses, can leak information to public critics. Investigative journalists can probe political surveillance. Citizens can expose what has happened to them. This is resistance aimed at mobilising wider awareness of surveillance and its damaging effects.

Many individuals attempt to avoid or disrupt surveillance, for example by giving incorrect information on forms, joining campaigns against identity cards, or damaging speed cameras. If actions are widely taken up, they can have a major impact and can stimulate development of new methods of resistance. Using and promoting encryption is an example. If everyone puts some encrypted files on their computer and sends occasional encrypted emails, even if they have nothing to hide, this makes it harder for snoops to determine who is worth watching. This is especially important in repressive regimes, where use of encryption might be seen as implying subversive activities. Struggles to enable access to encryption technology are a vital part of resistance (Schneier & Banisar 1997).

Gary Marx (2003) has distinguished 11 different types of individual resistance to surveillance, for example avoiding detection, blocking intrusive measures, refusing to provide information, and encouraging surveillance agents not to enforce regulations. He gives examples of each type of resistance and argues that there will be an ongoing struggle between controllers and resisters, with total control being unrealisable.

Methods of intimidation are often linked to cover-up. Beginning in the 1970s, *CovertAction Information Bulletin* challenged secret agencies by exposing the identities of undercover CIA agents; in response, the US Congress in 1982 passed a law against this. This law later led to a giant scandal when government officials revealed the identity of CIA agent Valerie Plame in reprisal against her husband Joseph Wilson for questioning false claims used to justify the 2003 invasion of Iraq (Wilson 2005).

This case suggests that data-gathering can sometimes be turned against powerful groups. Normally, the groups that instigate and run surveillance systems, such as politicians, employers, top bureaucrats and spy agencies, are not equally subject to the techniques they use against others. For example, employers may monitor workers but workers are seldom able to monitor employers to the same extent. Collecting data about the rich and powerful, putting them on a par with others, challenges and deters intimidation. In other words, if the rich and powerful want surveillance, then make sure the searchlight is turned on them as well as others.

7 Conclusion

In order to gain insight into struggles over surveillance, it is useful to analyse the methods typically used by perpetrators of perceived injustice to reduce outrage over their actions. The promoters of surveillance commonly hide their operations, denigrate the targets and critics of surveillance, give plausible justifications for operations, set up oversight bodies that have little power to challenge anything more than minor violations of regulations, intimidate opponents and provide incentives for cooperation. To refer to "promoters of surveillance" and describe their methods does not imply any conscious intent on their part: many of them do not see themselves as promoting surveillance, but rather as cracking down on crime, providing better consumer service or increasing the efficiency of service systems: they believe in their own interpretations of what is happening. Likewise, to speak about the methods used to reduce outrage need not imply any conscious strategy: these methods are simply intuitive or obvious ways to reduce opposition.

The value of looking at methods used by promoters of surveillance is that it gives guidance for opponents. Some of these are fairly obvious, including exposing abuses and explaining what is wrong with surveillance. Others are less so, in particular being sceptical of official channels and instead mobilising support. Over the decades, many critics of surveillance have advocated stronger regulations, yet these have been regularly superseded by new technologies, overturned by emergency powers, undermined by loopholes and made hollow by weak enforcement. According to the model used here — reflecting studies of a wide range of domains — relying on regulations is seriously flawed: to a considerable extent, it gives only the appearance of dealing with problems, dampening public concern while allowing developments to continue.

To challenge surveillance, according to the framework used here, public outrage needs to be fostered in a range of ways. The model gives guidance for actions that are likely to be effective, but it does not say who will or should take action. Dedicated opponents have too often been overwhelmed by the forces promoting surveillance. In such circumstances, even the best tactics may be inadequate.

Nevertheless, it is far too soon to lose heart. Many other social movements — against slavery, for women's emancipation, against environmental destruction — only gained widespread support after decades or centuries of exploitation and damage. Surveillance may become more ubiquitous and insidious, but there remains a strong reservoir of public concern about privacy, autonomy and freedom. Today's critics and campaigners are laying the basis for a future challenge to emerge. Understanding tactics can help make that challenge more effective.

Acknowledgements

I thank Gary Marx, Steve Wright and two anonymous referees for valuable comments on a draft.

References

Cowan, P, Egleson, N, Hentoff, N with Herbert, B & Wall, R 1974, *State secrets: police surveillance in America,* Holt, Rinehart and Winston, New York.

Dandeker, C 1990, *Surveillance, power and modernity: bureaucracy and discipline from 1700 to the present day,* Polity Press, London.

Davies, S 1996, *Monitor: extinguishing privacy on the information superhighway,* Pan Macmillan, Sydney.

Davies, SG 1997, 'Re-engineering the right to privacy: how privacy has been transformed from a right to a commodity' in *Technology and privacy: the new landscape,* ed PE Agre & M Rotenberg, MIT Press, Cambridge, MA.

De Maria, W 1999, *Deadly disclosures: whistleblowing and the ethical meltdown of Australia,* Wakefield Press, Adelaide.

Gandy, OH 1993, *The panoptic sort: a political economy of personal information,* Westview, Boulder, CO.

Garfinkel, S 2000, *Database nation: the death of privacy in the 21st century,* O'Reilly & Associates, Sebastopol, CA.

Holtzman, DH 2006, *Privacy lost: how technology is endangering your privacy,* Jossey-Bass, San Francisco.

Jasper, JM 2006, *Getting your way: strategic dilemmas in the real world,* University of Chicago Press, Chicago, IL.

Kimball, P 1984, *The file,* Allen & Unwin, London.

Lawrence, RG 2000, *The politics of force: media and the construction of police brutality,* University of California Press, Berkeley, CA.

Lyon, D 1994, *The electronic eye: the rise of surveillance society,* Polity Press, Cambridge.

Lyon, D 2003, *Surveillance after September 11,* Polity Press, Cambridge.

Martin, B 2005, 'The beating of Rodney King: the dynamics of backfire', *Critical Criminology,* vol. 13, no. 3, pp. 309-326.

Martin, B 2007, *Justice ignited: the dynamics of backfire,* Rowman & Littlefield, Lanham, MD.

Marx, GT 1984, 'Notes on the discovery, collection, and assessment of hidden and dirty data', in *Studies in the sociology of social problems,* ed JW Schneider & JI Kitsuse, Ablex, Norwood, NJ, 78-113.

Marx, GT 1988, *Undercover: police surveillance in America,* University of California Press, Berkeley, CA.

Marx, GT 2003, 'A tack in the shoe: neutralizing and resisting the new surveillance', *Journal of Social Issues,* vol. 59, no. 2, pp. 369-390.

Marx, GT 2007, 'Rocky Bottoms: techno-fallacies of an age of information', *Journal of International Political Sociology,* vol. 1, no. 1, pp. 83-110.

Moore, Jr., B 1978, *Injustice: the social bases of obedience and revolt,* Macmillan, London.

Murray, G 1993, *Enemies of the state,* Simon & Schuster, London.

Ogletree, CJ, Prosser, M, Smith, A & Talley, W 1995, *Beyond the Rodney King story: an investigation of police misconduct in minority communities,* Northeastern University Press, Boston.

Olmsted, KS 1996, *Challenging the secret government: the post-Watergate investigations of the CIA and FBI,* University of North Carolina Press, Chapel Hill, NC.

Roberts, A 2006, *Blacked out: government secrecy in the information age,* Cambridge University Press, New York.

Rosen, J 2000, *The unwanted gaze: the destruction of privacy in America,* Random House, New York.

Scarry, E 2003, 'Citizenship in emergency,' in *The Best American Essays 2003,* ed A Fadiman, Houghton Mifflin, Boston, 223-242.

Schneier, B & Banisar, D 1997, *The electronic privacy papers: documents on the battle for privacy in the age of surveillance,* Wiley, New York.

Sharp, G 1973, *The politics of nonviolent action,* Porter Sargent, Boston, MA.

Stalder, F 2002, 'Opinion. Privacy is not the antidote to surveillance', *Surveillance & Society,* vol. 1, no. 1, pp. 120-124.

Thomas, M 2007, '"Tony Blair is a cult"', *New Statesman,* 25 April, viewed 24 September 2007, <http://www.newstatesman.com/print/200704250005>.

Wilson, J 2005, *The politics of truth: inside the lies that put the White House on trial and betrayed my wife's CIA identity,* Carroll & Graf, New York.

RNSA
Research Network
Secure Australia

The Second Workshop on the Social Implications of National Security

From Dataveillance to Überveillance and the Realpolitik of the Transparent Society

29 October 2007
Wollongong, Australia

Editors: Katina Michael and M.G. Michael

Research Network for a Secure Australia
This event is organised by the Research Network for a Secure Australia (RNSA). RNSA is a multidisciplinary collaboration established to strengthen Australia's research capacity for protecting critical infrastructure (CIP) from natural or human caused disasters including terrorist acts. The RNSA facilitates a knowledge-sharing network for research organisations, government and the private sector to develop research tools and methods to mitigate emerging safety and security issues relating to critical infrastructure. World-leaders with extensive national and international linkages in relevant scientific, engineering and technological research will lead this collaboration. The RNSA also organises various activities to foster research collaboration and nurture young investigators.

Participants are encouraged to join the RNSA. Membership of the RNSA is open to Australian and international researchers, industry, government and others professionally involved in CIP Research. Information on joining is at www.secureaustralia.org.

RNSA

Convenor:	A/Prof Priyan Mendis, Head of the Advanced Protective Technology for Engineering Structures Group at the University of Melbourne
Administrator:	Mr. Anant Gupta, University of Melbourne
Node Leader:	Prof Joseph Lai, UNSW@ADFA
Node Leader:	Prof Ed Dawson, Queensland University of Technology
Outreach Manager:	Athol Yates

Editors: Michael, K. and Michael, M.G.
Publication Title: From Dataveillance to Überveillance and the Realpolitik of the Transparent Society (Workshop on the Social Implications of National Security, 2007)
Series: Research Network for a Secure Australia (RNSA)
Publisher: University of Wollongong, IP Location-Based Services Research Program (Faculty of Informatics) jointly with the Centre for Transnational Crime Prevention (Faculty of Law)
Contact Details: Tel 02 4221 3937, Fax 02 4221 4045, University of Wollongong NSW 2522
Conference Websites: http://www.secureaustralia.org/ & http://www.uow.edu.au/~katina/rnsa07.htm
Publication Year: 2007
Format: Book (hardcopy $50 AUD; softcopy $30 AUD http://www.homelandsecurity.org.au/publications.html)
Cover and text layout: Anthony Petre
ISBN: 978-1-74128-141-5 (print)
ISBN: 978-1-74128-142-2 (pdf)

Table of Contents