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., Dandekar 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 a cover-up. Such complaints procedures, once initiated, may threaten the police’s legitimacy (Ogletree et al. 2000).

On 3 March 1999, the police arrested George Holliday, who was filming the course of the Watts riot in Los Angeles. When footage was later made public, the reaction against the police’s cover-up and all the usual ways to avert the police’s interpretation of events. When Holliday’s supporters used cover-up, this time unusually, in this case, by using the _Daily News_ against the police.

Tactics for an attack on surveillance

The foundation for such an attack is at least some of the information, raw or with hidden value, being a tool of exploitation, and surveillance is a tool in opposition.

A sense of unfairness is generated and amplified by the psychic impact of a continual stream of dossiers and reports by purveyors of surveillance. These may amplify outrage against their actions and those attitudes.

Given that so much is damaging, there is some justification for more of the five methods. Towards the end of this paper, I look at examples of how to challenge these methods.

The five methods could be examined in detail, but an approach is to consider actors to be constrained by the real circumstances in which they conduct surveillance, though...

2 Cover-up and Devaluation

Surveillance is unlikely simply to happen, they
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 then the information is taken up by other people, some of them authorities with bad records.

3 Devaluation

If a person is not monitored, or if things are done so as not to be monitored, executing a serious crime at Guantanamo was dangerous for a significant number of people painted as terrorists at first.

It is to be expected that targets as a means of devaluing surveillance are used with a sufficient degree of fingerprinting without a conscious programme of monitoring of everyone.

Furthermore, developed democracies are said to be defended by surveillance.

The trite expression is built on an implicit ethical argument: you must have some control over your life (Kantor 2007). Therefore,

One way to control people is to monitor every individual, and to reveal through photos and personal details the nature of guilt at Guantanamo for being against government as a whole. Such revelations can generate concern,

Hicks’ father Terrence: ‘Lyn’. Mori: having value.

The same process, of devaluing individuals and changing them into targets, for example, Penn Kesey’s depiction of the US spy agency files an account of the process as a flimsy pretext. They are not enough to identify with the credibility of a spy agent who came in here. The process of surveillance gone too far. The arguments about this process have an analogy in Orwell’s novel 1984, another story of Winston...
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 be misused or out of control. They have challenged the field-based surveillance framework and argued that alternatives. And they have questioned justifications.

One of the most potent methods is the use of cameras. For example, cameras are widely seen as a safe deterrent to crime. But opponents? It is contested whether cameras are matched with people’s concerns and whether they provide more advantages, in particular in a group setting, or are an institutional problem.

John Gilliom argues that cameras are inappropriate drug testing in United States prisons in terms of safety at work. For example, cameras and other concerns are typically raised. Gilliom argues that rights are denied to the powerful, and that misuse of data is widespread. It is that opponents’ arguments are not in the interest of challenging tests.

5 Official complaints

Courts, ombudsman’s offices and official channels. This is where the process works, in a few cases, but where there are difficulties in channels typically publicised. The brave do not speak out in the public domain, but in practice these channels are typically colleagues, experts (such as lawyers and politicians), or the opposite of using public or semi-public bodies to protect privacy.

Some opponents of government have argued that which opposed systems is not so much an evidence, as an approach to government. They have argued that the amount of money spent on surveillance means that opposition options are not available or are not in favour of testing.

In Australia, the Australian Federal Police have received complaints of the abuse of information and the Commissioner has...
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 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 dissent and make it likely that activists can end up being hit a little bit safer, because the police are restricted in that case to more publicity).

There is also a range of other measures. If you are being watched, it is services. If you are being tracked, it is a licence number that goes with it. All comes along with some measure of greater willingness to provide information.

To oppose surveillance, you need to understand the knowledge that journalists can provide to the public, to give them an understanding of its damaging effects on freedom of speech.

Many individuals, like giving incorrect information, can be damaging specialists, can have a greater impact and can be found, promoting encryption and storing their computer anywhere they want out of sight, this makes individuals, and especially important figures, all the more important as implying subversion and disloyalty are a vital part of the opposition.

Gary Marx (1991) described surveillance, for example, as a form of information dislocation. He gives examples of the struggle between states and countervailing power.

Methods of Surveillance can be used for good or evil purposes. It depends on how it is used. The techniques that can be used by states and democratic nations are to protect their citizens, but workers are also targeted.
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, *Covert Action 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 for comments on a draft of this paper.

References

Westview Books
Bass, San Francisco
Marx, GT 1984, *Dirty dust and dirty data", JI Kitsuse, A
Marx, GT 2003,
Acknowledgements

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

References


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


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.


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


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.


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

Marx, GT 2007, ‘Rocky Bottoms: techno-fallacies of an age of information’,
Moore, Jr., B 1978, Injustice: the social bases of obedience and revolt, Macmillan,
London.
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.
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
Thomas, M 2007, “‘Tony Blair is a c*ck’”, New Statesman, 25 April, viewed 24
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.

Message communication as practice

Rob Nicholas1

1Consultant, 2Law

Abstract

This paper applies the concept of powers in practice to the area of the dynamic and
deficiency, carriers were capable of law introduced Bill in which the rationale
between the Attorney in the telecommunications
subsumed by the role the sector are respective interception and a

Keywords: lawful inquiry, assistance
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
Foreword

The 2007 Workshop on Research Network for a Secure Australia (RNSA) focused on the social implications of national security. The Research Network for a Secure Australia had been 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-leading experts 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.

The Workshop was organised by the Research Network for a Secure Australia. It provided a forum for researchers, academics or individuals interested in research and development activities in the field of national security. The workshop was hosted by the University of Wollongong and the Department of the Defence, Australia. It involved a range of participants from different fields such as history, politics, sociology, engineering, and technology.

The workshop included a variety of presentations and discussions on emerging issues related to national security. The presentations covered topics such as cybersecurity, resilience of critical infrastructure, and the social implications of national security policies. The presenters were also asked to submit their papers for publication in a special issue of the Journal of Homeland Security and Emergency Management.

Each paper was submitted by the presenters to the appropriate field for review and publication. The editors would like to thank them for their contributions and for the high quality of papers submitted. The editors also extend their thanks to the Defence Department and all those involved in supporting the workshop.
Table of Contents

1 Opening remarks ............................................................................................................. 7
   Doug MacKinnon
   Centre for Transnational Crime Prevention, University of Wollongong

2 A note on überveillance ............................................................................................... 9
   M.G. Michael and K. Michael
   School of Information Systems and Technology, University of Wollongong

3 Keynote address: What ‘überveillance’ is and what to do about it ...................... 27
   Roger Clarke
   Xamax Consultancy Pty Ltd

4 Keynote appendix: Surveillance vignettes ............................................................... 47
   Roger Clarke
   Xamax Consultancy Pty Ltd

5 Owning identity- one or many- do we have a choice? ......................................... 61
   Marcus Wigan
   Oxford Systematics

6 Opposing surveillance ............................................................................................... 71
   Brian Martin
   School of Social Sciences, Media and Communication, University of Wollongong

7 Message in a bottle: Stored communications interception as practised in Australia 83
   Rob Nicholls and Michelle Rowland
   Gilbert + Tobin

8 Australia and the ‘war against terrorism’: Terrorism, national security and human rights... 97
   Mark Rix
   Graduate School of Business, University of Wollongong

9 Panel session: The case for detention without charge in suspected terrorism cases in Australia 113
   Nicholas O’Brien
   Australian Graduate School of Policing, Charles Sturt University

10 The benefits and concerns of public data availability in Australia: a survey of security experts... 117
    Roba Abbas
    School of Information Systems and Technology, University of Wollongong
The Second Workshop on the Social Implications of National Security

11 Re-using public sector information (PSI) for profit: Who's data is it anyway? 129
   Mark Burdon
   Faculty of Law, Queensland University of Technology

12 The Internet as a communication medium and a social space: a social constructivist approach to the use of open data 147
   Lucy Resnyansky
   Defence Science and Technology Organisation

13 The Agora-Pnyx paradox 169
   George Mickhail
   School of Accounting and Finance, University of Wollongong

14 Something smart going on: the apocalyptic aesthetics of surveillance 181
   Marcus O'Donnell
   School of Journalism and Creative Writing, University of Wollongong

15 Auto-ID and location-based services in national security: Social implications 201
   Holly Tootell
   School of Information Systems and Technology, University of Wollongong

16 Privacy implications of automated GPS tracking and profiling 225
   Muhammad Usman Iqbal and Samsung Lim
   School of Surveying and Spatial Information Systems, University of New South Wales

17 Human tracking technology in mutual legal assistance and police inter-state cooperation in international crimes 241
   Katina Michael and Gregory Rose
   School of Information Systems and Technology and Centre for Transnational Crime Prevention, University of Wollongong

18 ePassport security under the microscope 257
   Matthew Sirotich
   School of Information Systems and Technology, University of Wollongong

19 Improving information security management: an Australian universities case study 281
   Tim Lane and Lauren May
   Faculty of Information Technology, Queensland University of Technology

Author Biographies 300

Opening talk

Doug MacKinnon
Director, Centre for Transnational Crime Prevention, University of Wollongong

Good morning everyone,

My name is Doug MacKinnon and I am the Director of the Centre for Transnational Crime Prevention and this is the Opening talk of the Second Workshop on the Social Implications of National Security.

In an age when globalisation has eroded national boundaries and disrupted the family and social structures, nation states and communities are facing a new threat: death and destruction on a scale that has not been seen since the Second World War, with maintaining peace of paramount importance.

Indeed the usual attempt to coordinate and communicate has failed and the cost is high.

The issue of crime is of critical concern to all countries, not only in the United States, where the legal profession is in the midst of a crisis, but also in Europe, where the threat of terrorism has led to the questioning of democratic values.

This has led to changes in the way that governments respond to crime and to the challenges of crime prevention.

The Australian Institute of Criminology (AIC) has been at the forefront of this change, providing a comprehensive picture of the social implications of national security.

The AIC's research and analysis provide an insight into the social implications of national security, providing a comprehensive picture of the current and potential future challenges faced by governments and communities.