Brian Martin
"Spying and surveillance," chapter 6 of
Ruling Tactics
(Sparsnäs, Sweden: Irene Publishing, 2017),
available at http://www.bmartin.cc/pubs/17rt/

6
Spying and surveillance

Spies: are they good guys or bad guys? The answer is easy: the spies on *our side* are good whereas the spies on *their side* are the worst of the worst.

Spying and surveillance are tricky for governments because of secrecy and obvious double standards. Let's look at some of the aspects and complications.

Spying on foreign enemies is the easiest case: it's assumed to be a good thing. However, to be effective, spying needs to be done covertly, so it's hard to praise spies in public. Furthermore, spying in general is often seen as a bit devious, so governments seldom boast that, "We have the best spies." Even mentioning the existence of current spies is a bit risky.

One solution is to praise past spying operations, done for a good cause. An example involves the Enigma machine, built in Britain during World War II to break Nazi secret codes. Breaking into codes is a type of spying, done at a distance, though it is perhaps better called surveillance. The story of the Enigma machine has been told in books and films, including the 2014 film *The Imitation Game*. It portrayed some British military figures unfavourably, with commanders being contemptuous of mathematicians and, after the war, showing serious bias against Alan Turing because he was gay. But this portrayal was in the overall context of the assumption that breaking German codes was a gallant, militarily crucial endeavour.

Very few people have personal experience of spying, or have even talked to a spy about what they do on the job. Consequently, ideas about spying are largely shaped by media coverage, much of it fictional in novels and films. In the widely read novels by John Le Carré, most of them set during the cold war, the world of spies is deceptive and morally challenging, with agents, double agents and double crossing. Overall the impression is that spying is somewhat disreputable. Indeed, spying requires lying, and thus has a taint about it.

Perhaps for this reason, as well as operational secrecy, governments say little about their own current spies. But when it comes to foreign spies, it is another matter: they are mightily condemned. (In practice, many foreign spies are monitored but never exposed; some are quietly expelled.) A few are arrested, tried and given long prison sentences, worse than if they had committed murder.

The most severe condemnation is reserved for insiders who serve the enemy: citizens, who are supposed to be loyal, who sell secrets or, even worse, reveal secrets because they believe in the cause of the enemy. Spying is cast into the mould of us versus them.

However, old-fashioned spying using agents has long been superseded by signals intelligence, which involves surveillance of electronic communications. All sorts of sophisticated techniques are used to monitor phone calls, emails and every form of electronic communication. Mostly this goes on in secrecy by all involved. Occasion-

ally, though, there are stories about foreign dangers, for example hacking into databases by agents on behalf of North Korea or China. Because of secrecy, media stories are untrustworthy. Foreign governments seldom fess up saying "Yes, we were trying to access your vital data." Informed observers are wary: media stories may be due to strategic leaks intended to serve political objectives.

Some ways to refer to an agency

National security agency	This is the most serious-sounding terminology, implying grave responsibility. This is the most overtly state-oriented expression.
Intelligence organisation	The word "intelligence" has positive connotations because of the more common usages of the word, so this is a favoured expression by supporters of these organisations.
Surveillance operation	This emphasises a potentially negative side to agency activities.
Spy agency	This has negative connotations, given that spying is often seen as somewhat underhanded.
Secret police or political police	These terms highlight the capacity for political repression, and point to a connection with dictatorial regimes.
The spooks	This is an informal, humorous term.

A lot of surveillance is about economic information, for example trade secrets, designs and plans. Supposedly every government with suitable capacities does this, but it is usually kept secret. Occasionally there are popular cries to stop foreigners from "stealing our secrets," as though only foreigners engage in commercial espionage.

Then comes the most challenging surveillance of all: a government spying on its own citizens. In police states, this is a means of keeping control by monitoring dissent. In the former East Germany, the Stasi—the feared secret police—received information from one out of ten citizens in one of the most pervasive monitoring systems ever known. In the west, this sort of surveillance is condemned, so it is not surprising that western governments' own surveillance of their citizens is carried out in utmost secrecy.

Thinking in terms of in-groups and out-groups, there are two sets of processes going on here. Governments seek to build loyalty by encouraging citizens to think of themselves being part of a loyal in-group, and can foster this by creating, exaggerating or stigmatising out-groups. Foreign enemies are prime candidates for being out-groups and for bolstering in-group solidarity. Terrorists serve the same function, especially when they are seen as foreign or alien. But what if some of the "enemy" are actually part of "us"? This makes things trickier. The internal enemy could be communists, capitalists, ethnic groups, religious groups and so on. The risk to the government is that its own agents, including ones undertaking surveillance, will come to be seen as the enemy.

Consider the former Soviet Union, in which people were encouraged to report family members who were

enemies of the state. For those who did this, one reward was greater identification with the state: for them, the out-group was class enemies. But for others, family loyalties were greater, and attempts by the government to encourage spying caused questioning of the state itself: for them, the state became an out-group.

Only in some circumstances can groups create loyalty that outweighs all competing loyalties. One of the reasons for the celibacy of priests in the Catholic Church is that it removes a competing source of loyalty: wives and children. Some cults require celibacy whereas others break down personal loyalties by expecting or mandating sexual relations with many different partners.[1] Governments have seldom been able to break down family loyalty; when they try, they risk being seen as the enemy of the people.

The governments of Australia, Britain, Canada, New Zealand and the US for decades had an intelligence-sharing arrangement called the Five Eyes agreement. Secret monitoring stations were set up to collect every possible electronic communication, and software developed to search the resulting data. This operation was so secret that its existence was hidden from the public, and even its name, Echelon, was secret.

New Zealand campaigner Nicky Hager made the first major breakthrough. Through conversations with workers at the facility at Waihopai run by the Government Communications Security Bureau, the New Zealand government's signals intelligence agency, he gradually

1 Lewis A. Coser, *Greedy Institutions: Patterns of Undivided Commitment* (New York: Free Press, 1974).

pieced together more and more information. The more information he obtained, the more he was able to suggest he knew more than he did, and thereby gather additional information. His 1996 book *Secret Power*[2] became well known among those who followed the machinations of government spy agencies, who also read James Bamford's *The Puzzle Palace* about the US National Security Agency and related exposés.[3] Hager's discoveries received some publicity when in the late 1990s repression-technology expert Steve Wright wrote about the Echelon surveillance system in a report to the European Parliament.[4]

Wider public awareness of massive western government surveillance of their own citizens did not occur until Edward Snowden's massive leak of documents from the US National Security Agency—the lynchpin agency in the Five Eyes agreement—hit the news in 2013.[5] Snowden's amazingly detailed information overshadowed previous

2 Nicky Hager, *Secret Power: New Zealand's Role in the International Spy Network* (Nelson, New Zealand: Craig Potton, 1996).

3 James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency* (Boston: Houghton Mifflin, 1982).

4 Steve Wright, "The Echelon trail: an illegal vision," *Surveillance & Society,* Vol. 3, Nos. 2/3, 2005, pp. 198–215.

5 For informative accounts, see Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA and the Surveillance State* (Hamish Hamilton 2014); Michael Gurnow, *The Edward Snowden Affair: Exposing the Politics and Media Behind the NSA Scandal* (Blue River Press, 2014); Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (Guardian Books 2014).

findings, which were for the most part forgotten or ignored. The evidence was clear: massive government surveillance, carried out in supposedly democratic countries, was standard practice, not only against foreign enemies but also against ordinary citizens. It was bad when done by the East German Stasi. Why was it okay in the US?

Whereas previously the spying had been kept out of the public eye, not just for operational reasons but to prevent outrage, now it needed to be explained and justified. For governments and their apologists, a series of rationales emerged. One was to attack the messenger, calling Snowden a traitor. Another was to say, as had been said many times before, "If you've got nothing to hide, you have nothing to fear," implying that only criminals and terrorists should be concerned about government surveillance. There are many replies to this presumption in the form of a question. One of the easiest is to say, "In that case, please give me your credit card numbers and passwords."[6]

Governments can try to justify surveillance through the usual us-versus-them dichotomy, assuming surveillance is entirely against enemies of the state and people. The trouble is that many citizens start distrusting the state itself. This is apparent in the popularity of 9/11 conspiracy theories. Setting aside the question of whether President George W. Bush or other US officials actually had

6 Actually, the issues are more complicated than this. See Daniel J. Solove, *Nothing to Hide: The False Tradeoff between Privacy and Security* (New Haven, CT: Yale University Press, 2011).

anything to do with the planning or execution of the attacks on 11 September 2001, that so many people believe they might have suggests a deep-seated distrust of the US government.

Then there is the role of US spy agencies in other countries: they often team up with repressive governments, in particular with security forces involved in surveillance, arrests, torture and killings. For example, rage in Egypt against President Hosni Mubarak, who stepped down in 2011 following massive protests, was in part directed against his ruthless security apparatus and, by association, US partners.[7] So there is an international dimension to outrage over spying on citizens: when governments share intelligence information against alleged enemies, this can undermine trust among citizens who know about it.

Secrecy and surveillance

Scott Horton in his book *Lords of Secrecy* provides a powerful indictment of secrecy in US agencies involved in spying and surveillance. Horton argues that public discussion is essential for a democratic society, citing the example of ancient Athens, where citizens were involved in important decisions, including about security, namely going to war. Ancient Athens was successful in relation to its more authoritarian rivals, such as Sparta, because it was a "knowledge-based democracy," gaining strength from

7 Scott Horton, *Lords of Secrecy: The National Security Elite and America's Stealth Warfare* (New York: Nation Books, 2015), p. 157.

sharing and debating ideas from many individuals and sectors of society.

Horton traces the rise of excess secrecy in the US to the emergence after World War II of the national security elites, who dealt with nuclear weapons development and the challenge from the Soviet Union. He says the problem of unaccountable power was recognised by President Harry Truman and senior advisers who set up the Central Intelligence Agency; they established oversight mechanisms via the legislative branch of government, namely Congress. However, according to Horton, the huge size and resources of the spy agencies, combined with their use of secrecy, before long overwhelmed and captured their congressional overseers. Secrecy became a tool to build bureaucratic empires, to hide failures and to carry out policies without scrutiny.

The next sector of society with the potential to restrain the agencies was the media, but the US mass media became tools of the state, being reluctant to break stories about any sort of abuse, for the example the 1968 My Lai massacre in Vietnam or the torture at Abu Ghraib prison revealed in 2004. So, according to Horton, the one remaining group with the potential to challenge unaccountable secrecy is whistleblowers, who have become a target for suppression.

Horton's analysis points to the powerful role of secrecy in agencies involved in spying and in undeclared war, in particular the use of drones for extra-judicial assassination. Secrecy can become an end in itself. Horton himself is not making an argument against surveillance or drones or wars. He just wants there to be an open discussion so that better informed decisions, with support from politicians and the public, can be made.

This is enough background to indicate the complexities of spying and surveillance in relation to building loyalty to the state. Basically, the government has to pursue seemingly contradictory directions, maintaining secrecy for operational reasons and to hide corruption and abuses, while somehow convincing members of the public that monitoring them is for their benefit.

In the following sections, I first outline tactics to build loyalty to the state in relation to spying and surveillance, then tactics against alternatives to the standard approach, and finally tactics to challenge surveillance.

Tactics to build loyalty

The first tactic is *exposure* of good things about the state. Here the challenge is the greatest. The safest approach is to expose only achievements, such as spying successes in past wars and successes in preventing terrorism. However, this has to be done carefully so as to suggest that bad guys are the only targets. By carefully picking stories to release, and angles on those stories, the aim is to encourage people to *value* the role of intelligence services, positioning them as protectors of the population.

Their role is *explained* as a necessary function of maintaining security. Part of the explanation involves suitable framing. Rather than refer to spying and surveillance, the usual language is of intelligence and national security.

Governments routinely *endorse* their intelligence agencies, and *reward* them generously with good salaries

and conditions, as part of ample budgets that signify the importance of their task.

In these ways, governments try to build citizen loyalty to the agents of control. However, compared to many other areas—museums, elections, sport, education, media—the task is greater because spying itself is often seen as a shady sort of activity, involving deception and underhanded methods. It's a bad method of achieving a good goal, and the negative associations with the method tend to rub off on the goal. So for many governments, the less said the better. Justifications are only brought forth when the issue has been publicised or when arguing for greater resources. Their ideal technique is to condemn spying by other governments and hope that no one even thinks about their own spying.

Marginalising alternatives

Are there any alternatives to the usual government spying? This is a difficult question to answer, because there is so little discussion of alternatives. Let's consider some possibilities.

One alternative is to say there should be no spying at all. This is easy to challenge, because the bad guys—foreign governments—are spying on us, so we need to spy on them. So the no-spying option is usually posed as, "There should be no spying on our own people." This is actually a radical alternative in countries where the government is repressive and nearly all surveillance is against internal opponents. To this option, governments regularly use the method of fear-mongering, raising the alarm about terrorists, communists, traitors, heretics or

others who threaten the fabric of society, in other words the government.

There are, in some cases, actual opponents who pose some danger to the public: terrorists and criminals for example. Such opponents are valuable for governments because they help justify spying on everyone. For the moment, assume there are legitimate reasons for surveillance. How should it be done?

The usual approach is to have a system but make sure it is under legitimate political control, for example with scrutiny by elected politicians, who supposedly serve as agents of the public. The trouble is that spy agencies become too powerful and can win over their political masters, invoking the necessity of secrecy to ensure that effective controls are seldom invoked. On a more nasty level, spy agencies can collect dirt on politicians, implicitly threatening to covertly release the information. The FBI under J. Edgar Hoover supposedly engaged in this sort of blackmail. It is the sort of technique used by criminal organisations: demand participation in crime and then use the possibility of exposure to deter disloyalty.

So what about alternatives that involve something completely different? One possibility is promoting social justice. Rather than spying on opponents, instead address the sources of their grievances. This is good for a long-term view, but does not address the possibility of immediate threats.

One alternative is to introduce a "citizens inspectorate," namely citizens who have the power to check what spy agencies are doing and to make reports and recommendations. To be effective, a citizen inspectorate

would need to be sizeable and have a significant turnover to prevent capture by the agencies.

Some agencies already have an oversight body or individual, for example an inspector-general to whom complaints can be made by employees or members of the public. The trouble with such systems is that they usually become closely aligned with the agency, the same problem that occurs with legislative oversight.

If citizen inspectors were randomly chosen and served short terms, they would be less likely to be able to bought off or intimidated: some of them might be independent enough to make probing assessments and discourage abuses.

Agency heads would detest such a proposal, no doubt arguing that citizen inspectors, lacking security clearances, could not be allowed to know what agencies are doing. This objection is the familiar claim that secrecy prevents scrutiny.

Another alternative would be to set up a secure avenue for leaks from agencies. By analogy with WikiLeaks, it might be called SpyLeaks. This would enable abuses to be exposed with less likelihood of reprisals. Then comes the question of who would have access to the leaks. Perhaps legislators, or citizen inspectors, or even the general public.

Given the efforts of the US government to shut down WikiLeaks, it is obvious that SpyLeaks would never get off the ground. If it were ever implemented by agencies themselves, it might well have a back door so that agency officials could identify the leakers.

Giliam de Valk and I wrote an article about "publicly shared intelligence."[8] Giliam in his PhD research compared the performance of the Dutch intelligence services, which operated with the usual secrecy, with a very different sort of intelligence operation: the Shipping Research Bureau. The Bureau operated at the time of apartheid in South Africa, when there was an international embargo of oil imports as a form of pressure against the regime. However, some companies broke the embargo, sending their ships surreptitiously to deliver oil to South Africa. The Bureau sought to collect information about these rogue traders and expose them, thereby shaming the companies.

The Bureau used secrecy in some aspects of its collection and analysis of data. Individuals sent the Bureau information about ships, and it sought to verify this information, but did not release the names of its informants. But the Bureau's reports were public. Unlike spy agencies, it made its assessments available for scrutiny.

Giliam in his research found that the Bureau's reports were far more accurate than reports of the Dutch intelligence agencies. Publicly shared intelligence apparently had an advantage. This was what you might expect: open scrutiny improves quality. The same thing happens in science. The quality of the open scientific literature, which is subject to peer review before publication and available for scrutiny by anyone after publication, is widely

8 Giliam de Valk and Brian Martin, "Publicly shared intelligence," *First Monday: Peer-reviewed Journal on the Internet,* Vol. 11, No. 9, September 2006.

regarded as superior to secret corporate or government research. Similarly, open source software, in which the code is publicly available for scrutiny, is usually superior to proprietary software.

Publicly shared intelligence thus offers an alternative to the usual government surveillance. By drawing on the resources of the entire population both for inputs and evaluation of assessments, this form of intelligence would have the advantages of open source alternatives. (We didn't call it open source intelligence because that name was already used for a different alternative: intelligence drawing on openly accessible information, but lacking the open scrutiny essential for quality control.)

Publicly shared intelligence would be a frontal challenge to conventional intelligence operations built around secrecy. As expected, there has been no government interest in this alternative. For all practical purposes, it is invisible. No government has sought to test it.

From this brief discussion of ways to provide stronger oversight of spy agencies, it should be obvious that agencies will do nothing to publicise options that enable significant independent citizen involvement, much less actually implement them.

Challenging government surveillance

A key method of challenging surveillance is to expose it. Secrecy serves spy agencies by hiding abuses and failures. The bigger the abuse, usually the greater the secrecy.

Whistleblowers, leakers, investigators and journalists play crucial roles. Edward Snowden revealed unparalleled amounts of inside information. He was highly effective

because he kept a low profile until he had gathered the information. (He kept his plans secret.) He then carefully chose a journalist and media outlet—Glenn Greenwald of the *Guardian*—to whom to release the information. When Greenwald wasn't responsive, Snowden contacted Laura Poitras, a dissident filmmaker and friend of Greenwald's, and arranged to meet them. Snowden chose well: the *Guardian*'s editors refused to buckle to pressures from the National Security Agency and its British equivalent, and went ahead with exposé after exposé.

Another exposure technique is to reveal the identities and activities of spies. The magazine *CovertAction Information Bulletin* beginning in 1978 published the names of a number of CIA agents. So effective was this outing that in 1982 the US Congress passed a law making such disclosures illegal and subject to severe penalties. This response suggests the power of exposure: spies aim to gather information about others but they don't want information gathered about themselves: their efforts rely on secrecy and deception, for example false identities.

Today, it is far easier to collect and publish information. Citizens with digital cameras can record police use of force as it happens, in many cases exposing abuses that in previous decades would have been hidden from the public. Similarly, recording of the identities and activities of spies can be a powerful technique.

Another important technique is to counter the justifications for surveillance. This is a big area. One technique used by agencies is to lie about the value of information gathered, for example in preventing terrorist attacks. Critics can expose the failures of agencies, for

example in not picking up on clues about the 9/11 attacks or not anticipating the Arab spring. There were important failures decades ago too, for example the falsity of the alleged "missile gap" between the US and Soviet nuclear arsenals in the late 1950s, and the failure to anticipate the collapse of communist regimes in 1989. These were all failures of US agencies; there would be equivalent shortcomings in agencies in other countries that need to be exposed and criticised.

Next is the issue of official channels. Many governments establish laws and regulators for privacy protection. In practice, though, these seldom do much to control surveillance operations. Indeed, there is a body of writing on how privacy protection is routinely outflanked by technological developments and rogue operations.[9] What does privacy legislation do in the face of ever-expanding use of security cameras? What about revenge porn, when people post sexual images of former sexual partners? What about the Five Eyes surveillance of citizens?

Most employees tasked with enforcing privacy laws and regulations do their best, and no doubt many worthwhile protections have been implemented. But this is a losing effort in the face of an onslaught of monitoring capacities, including ones where people voluntarily offer information that potentially can be used against them, mostly in social media, also subject to monitoring and analysis by governments.

9 For example, Simon Davies, *Monitor: Extinguishing Privacy on the Information Superhighway* (Sydney: Pan Macmillan, 1996), chapter 6.

Rather than rely on privacy protection to limit surveillance, a more promising approach is to mobilise support, indeed to build a social movement. But despite people's serious concerns about government surveillance and many abuses, there is little sign of the development of a broad-based anti-surveillance movement.

There are many initiatives. The group Anonymous has taken direct action online in support of WikiLeaks. There are many supporters and users of encryption who oppose efforts by US government officials to mandate backdoors to encryption systems using the rationale of needing to be able to track down terrorists. Then there are software developers and entrepreneurs making accessible the means to avoid surveillance. These include the developers and promoters of the Tor browser, search engines like duckduckgo that do not record searches, convenient encryption systems and anonymous remailers, among others. A basic test is to ask, "Would this system be useful to dissidents in a repressive regime?" If it is, then it is probably worth promoting everywhere, including in countries where governments ostensibly respect civil liberties, because when it comes to surveillance, lots of governments are seeking powers that can easily be used to suppress dissent—and quite possibly are, given the secrecy involved in the whole system.

Part of challenging surveillance is resisting it, and that is not easy in a world with ubiquitous monitoring. It's possible to keep a low profile, but this might involve considerable inconvenience, for example not having a credit card, not driving (in areas where vehicle licence numbers are monitored) and not using a mobile phone.

Another form of resistance is to insert incorrect information into databases, for example "accidentally" using a slightly different birthday or address for different databases, or perhaps some politician's phone number. Although this can make it more difficult to collate data about you—you may end up with lots of nearly identical but slightly different versions of yourself on databases—it does little about surveillance more generally. Fake profiles on Facebook, Google and other platforms are common, many of them manufactured and sold to enhance the buyer's online image.

Because remaining outside routine surveillance is so difficult, and putting false information into databases usually has a marginal impact, probably a better form of resistance is to make public statements or otherwise protest surveillance openly. Some opponents set out to disable security cameras. Others perform colourful protests in front of the cameras for the delectation of operators.

Spying and patriotism revisited

There are various ways to oppose spying operations, but how do these relate to state power? To start, much surveillance is undertaken by the state, so opposition directly challenges state power. Other surveillance is undertaken by companies, for commercial purposes. Facebook and Google collect information about users to better direct advertisements, the lifeblood of their operations. However, as Snowden's leaks revealed, spy agencies use various means to tap into private information streams.

Probably just as importantly, private data collection makes people become used to exposing their lives online,

without thinking about how data is being collected by banks, phone companies and social media companies. Surveillance is increasingly seen as normal, as nothing much to worry about. When people regularly reveal details about their lives to anonymous companies and government agencies, they are likely to come up with rationalisations to justify what they do. This helps explain why anti-surveillance has not become a major social movement.

However, governments are still caught in their own contradictions. They undertake surveillance, but want to keep it secret and therefore have difficulty justifying it when it is exposed. They want to make people believe that all spying is on bad guys, but then are exposed spying on their own citizens. So they point to the dangers of criminals and terrorists, but at the risk of becoming tainted by their association with internal spying, often associated with repressive regimes.

Government thus can have a hard time finding the optimal balance between hiding and justifying their spying operations. Surveillance is not a good means for them to drum up support. Opponents can use the inherent contradictions in state surveillance in mobilising resistance, but have their own challenges in trying to get people to care enough to act, given the gradual encroachment of data-gathering methods and the immediate benefits to individuals in acquiescing to this data-gathering.

Perhaps the most powerful technique is to use the expanded capacities for collecting data against government agencies themselves. Already, police are changing their behaviour because of the ubiquity of cameras recording their actions. Perhaps government officials may

decide to change their operations if they start becoming the target of citizen surveillance.