SURVEILLANCE: TECHNOLOGICAL CHANGE, FOREIGN PRESSURES AND OVER-REACTION TO TERRORIST THREATS

Nicky Hager

All civil liberties must be balanced with other legitimate rights and needs of society. My rights must be balanced with other peoples' rights. The right to personal privacy must be balanced with society's need to investigate serious crime. Freedom of movement with road safety and civil aviation regulations. And so on.

In each case the question needs to be asked whether the legitimate needs of society and upholding some people's rights are a good enough reason to restrict other's rights. A free society is built upon working constantly to get this balance right and, if there is uncertainty, erring on the side of protecting civil liberties.

Compared to much of the world, New Zealanders have the good fortune of living in a very safe and free country. Unfortunately, this can have the effect of making people complacent and unobservant about threats to civil liberties.

In my opinion, New Zealand is going through a period of serious degradation of civil liberties. Some expansion of surveillance may be justified but most is occurring without any objective necessity, driven by technological change, foreign pressures and over-reaction to terrorist threats. We still have a much freer country than many, but when we consider the dramatic reversal of decades-old civil liberties occurring in the United States (before and after 11 September 2001), we should not take our relatively fortunate state for granted.

To date the negative changes to civil liberties in New Zealand have barely registered as a subject of public debate, partly because the impact is not felt acutely by middle class pakeha New Zealanders and more recently because exaggerated threat assessments following September 11 have dominated policy discussions.

Another possible reason for the lack of debate is that state surveillance powers have been increased with the support of the Labour Party (in opposition and then in government), a party traditionally relied on by the public to defend civil liberties. Currently that party, in government, appears to include no one who is seriously interested in privacy and other civil liberties.

The following list shows the breadth of changes occurring.

NON-STATE SURVEILLANCE

1. Surveillance at work

There has been a rapid increase in monitoring of employees within their workplaces, to a point where some highly intrusive practices are starting to seem normal. Some examples

are:

- Employers monitoring staff e-mail and phone logs
- Closed-circuit TV (CCTV) monitoring of employees in workplaces
- Electronic bugging of employees. A recent case I've heard of is a food processing company in Levin where, unbeknown to the staff, their conversations in the lunchroom are monitored by the company management.

2. Surveillance at home

There is a growing industry in surveillance technology designed for some family members to use against others (parents against children, husband against wife etc). Some are marketed as protection for children, others purely for snooping.

- Hidden CCTV cameras and Internet and e-mail monitors are available for suspicious partners and for parents.
- Toys and other household objects can be purchased containing surveillance equipment. There is a massive growth in the types of surveillance equipment freely available.

3. Surveillance by private firms

Private investigators and private security companies have all manner of electronic surveillance tools available to assist their clients. Huge holes in existing privacy laws, and the difficulty of policing even the existing protections, mean that people snooping for profit operate widely, within and outside the law.

4. Commercial surveillance / Data surveillance

There has been a huge increase in the collection, analysis and selling of personal information for commercial purposes. This growth has accompanied the growth of electronic data sources (sales and checkout data, mortgage information, loan and debt information and so on). Analysis of these sources provides aggregated data to assist marketing companies, but can equally provide information about individuals (monitoring their "data trail"). As more and more data sources become available and are combined, the intrusiveness of this activity will grow. For example:

- Flybuys is promoted purely as a loyalty scheme, but it involves written agreement to the collection of large amounts of personal spending information that is linked to the individual (and the biographical details they provide) by their card.
- Baycorp puts together an ever-wider set of data sources such as individuals' loans and debts, addresses and other personal information. The result is a privately-compiled database of information about most New Zealanders that is freely available to Baycorp's customers.
- Also, there has also been little thought about the widespread CCTV monitoring of people in places like shops and petrol stations – and the possible future face recognition, aggregation and analysis of this data.

5. Street surveillance

The concept of a "public place" is changing subtly but very significantly with the increasing use of surveillance systems.

- There is rapidly increasing use of CCTV monitoring of streets, train and bus stations and parks. Various British cities have already supplemented their CCTV systems with face recognition technology. Other systems use computer programmes to notice unusual patterns of behaviour in monitored areas.
- Automated surveillance of car number plates is not far behind the CCTVs. Whether it is introduced for traffic or crime reasons, this will have profound effects as it monitors the movements of many citizens.
- The next step would be centralised monitoring facilities where surveillance data would be stored for future use and where databases of faces and number plates would be stored. For instance, the *New York Times* of 14 March 2003 reports that the State of Illinois Department of Motor Vehicles has a database of 13 million face images, used (presumably among other things) to spot individuals seeking multiple licenses under different names.
- Justified as crime detection measures, CCTVs and face recognition technology have the potential to eliminate privacy in public places as every citizen is routinely monitored. There has been little debate about the claimed benefits and long-term costs of these developments.

Notice that many of these surveillance changes are technology driven as opposed to arising from some pressing social need. Digital technology has made all kinds of surveillance possible that was previously unimaginable or at least far more difficult or expensive. New devices and systems are developed and manufactured in other countries then gradually find their way here. There is an urgent need to find the proper balance between individuals' civil liberties and the assumed value of this surveillance.

Just as unauthorised monitoring of people's spoken communications is illegal (reflecting the state of technology when the laws were written), new privacy laws are urgently needed to maintain legitimate privacy in the digital age. For instance, in September 2002 a British MP announced that he will introduce legislation stopping monitoring of staff e-mail by employers. Technical ability to conduct surveillance should not be seen as a license to do so.

Priority should be given by the Government to developing comprehensive new privacy legislation for New Zealand.

STATE SURVEILLANCE

State surveillance activities in New Zealand are also partly technology driven. But the biggest influence by far is the expectations of and requests from allied countries, particularly the United States and Britain. Most activities of New Zealand's intelligence agencies, most surveillance legislation and most technology are the direct result of the so-

called "long standing intelligence relationships".

Partly the result of technological opportunity and partly reflecting a swing against civil liberties in the US and Britain (well before the 11 September 2001 attacks), a series of intrusive new surveillance plans have appeared in those countries in the last decade. A few years after their adoption there, we often hear that similar moves are being considered in New Zealand as well.

One example of foreign pressures I have followed concerns two pieces of surveillance legislation currently before our Parliament. Changes to the Telecommunications Act, introduced to Parliament in November 2002, will impose legal obligations on telecommunications companies to co-operate with surveillance of their customer's communications, including real time access to e-mail, text messages and mobile phone communications under an interception warrant. The Crimes Amendment Bill No. 6 will give the Police and SIS new powers to conduct these new forms of surveillance and also to hack into individuals' computers.

Although these bills are being put through Parliament in a post-September 11 climate, they date from a decade ago when the United States Government pushed through very similar legislation (against major protest from US civil liberties groups). I became aware of these moves when I learned that New Zealand Police and Security Intelligence Service staff were part of international working group meetings in Europe looking at new surveillance capabilities. These meetings were initiated by the US Federal Bureau of Investigation in 1993 and involved the FBI trying to persuade European Union countries (and others such as Australia, Canada and New Zealand) to adopt surveillance laws like the US one. The US goal is a standardised international surveillance regime that allows people of interest to the US authorities to be monitored across many countries.

In October 2000 I wrote an article predicting that legislation based on the FBI-EU negotiations was going to appear soon in New Zealand. Minister Paul Swain confirmed that the legislation was coming but denied there were any links with international surveillance planning. It was, he said, a "conspiracy theory".

Since then I have obtained many of the background papers under the Official Information Act. The New Zealand Police documents clearly show the attendance of New Zealanders at the FBI-EU planning meetings (called the International Law Enforcement Telecommunications Seminars, ILETS), records of commitments the New Zealand officials made at those meetings and then meetings in the late 1990s where the officials proposed the legislation changes to the relevant National Government Minister. There was apparently no sense of urgency, with regular reminder letters arriving from the ILETS secretariat over a number of years reminding the New Zealand officials of the undertakings they had made. Finally the Labour Government agreed to introduce the legislation we see now before Parliament.

Mostly these foreign linkages are not made public. However in my experience many initiatives in New Zealand concerning policing and intelligence, immigration, customs and civil aviation can be traced back to plans emanating from and commitments made to the relevant (usually US-dominated) international organisations or US and British agencies.

The expansion of legislative powers and technical capabilities for state surveillance of New Zealand citizens has several main features:

- The insidious trend for technology and practices developed by intelligence agencies (for national security threats) to be used for targeting ordinary citizens (eg. for policing crime and protest). Likewise the equally insidious use of military-style tactics developed for fighting wars and counter- terrorism for all manner of domestic policing roles (notably our police's para-military Special Tactics Group). These trends are occurring despite statistics showing consistent declines in reported crime and the absence of political violence in New Zealand.
- Virtually all the new surveillance powers and capabilities are direct imports from the US and Britain.
- We can reasonably predict – based on experiences in other countries – that the increased powers and capabilities will lead to higher overall levels of surveillance, despite a lack of evidence of increasing threats to justify the eroding of civil liberties.
- The introduction of new state surveillance powers and capabilities is surrounded by secrecy and carefully managed public relations – minimising rather than encouraging public debate. The public is not getting any effective say on the changes occurring.

Increasingly, in a re-run of Cold War thinking, the rationale for new security/surveillance moves is not to protect New Zealanders but because of the tenuous concern that New Zealand not be able to be used as a base for criminal or terrorist actions against the US and other allies. This is also the basis for the ILETS-co-ordinated standardisation of surveillance laws. In other words, New Zealander's civil rights are being reduced because of security fears of other countries.

Based on developments in Britain and the US, there are various surveillance initiatives that it is likely our Government will be under pressure to introduce in the coming years:

- Legal requirements on telecommunications companies to store records of every customer's phone calls, mobile calls, e-mails, faxes and Internet usage for, say, one or two years (or longer) – that is, "traffic data" showing who each customer's communications were to and from, when and for how long – and to make this data available to intelligence agencies and police. EU countries have recently bowed to pressure to do this.
- Biometrics (eg fingerprints or images of a person's iris) on passports. The US has been pushing hard for this in fora such as the International Civil Aviation Organisation. Our government has already agreed to it.
- Legal powers to obtain location data from telecommunications companies for individuals' mobile phones.
- Personal identity cards that all citizens would be required to carry – that telltale sign of societies with poor civil rights. There is currently renewed pressure in Britain and the US to introduce identity cards and so similar pressures can be expected here. Identity cards, like biometric identity systems, are an essential basis for enhanced surveillance systems for large-scale tracking and monitoring of individuals. For instance, the US is developing a system of registration for all Middle East immigrants – something that

would have been unthinkable in that country until recently. It will be a small step to having all their faces and other biometric data in surveillance systems throughout the country.

- Centralised surveillance centres that combine data from an ever-increasing range of sources to monitor individuals. ID cards and biometric identification of individuals, car license plate monitoring, CCTV monitoring, communications data collection are all steps in this direction. Advances in technology make this sort of centralised surveillance centre feasible and so – unless privacy and civil liberties concerns gain greater attention than they are at present – police and intelligence agencies can be expected to maximise their surveillance capabilities in this way.

Any time you talk to people involved with privacy and civil liberties in the US and Britain, there is news of more initiatives in their countries that may also turn up here. For instance, current British Labour Government moves include greater data sharing between government agencies, compulsory genetic samples being taken off anyone arrested for any crime, smart ID cards for immigrants including digitised thumbprint and government funding for expanded local authority CCTVs.

I am sure I have missed lots of areas, but the pattern is clear. Technological developments combine with foreign pressures to create a constant push for more surveillance. With each step, proponents (including Labour Ministers here) use the facile argument, direct from police states, that "if you're doing nothing wrong you have nothing to fear from surveillance".

These developments require New Zealanders to take civil liberties much more seriously. This includes rethinking the traditional approach of following the US and Britain. At a time when the retiring Republican House majority leader in Congress Dick Armey says he believes US Attorney-General John Ashcroft and the Justice Department are "out of control", New Zealand should stop using the United States as the role model for planning and decisions on these matters.

EXAGGERATION OF TERRORIST THREATS TO NEW ZEALAND

Vague claims of terrorist threats, like the communist threat of earlier decades, are a powerful tool to justify more repressive security, immigration and policing policies. The third major factor in the current degradation of privacy and civil liberties in New Zealand, besides technological developments and foreign pressures, is the government and news media over-reaction to supposed terrorist threats. It is worth looking at the current reaction to terrorism in detail.

The current political climate in the US resembles the anti-communist hysteria of the early Cold War. The September 11 attacks, and subsequent fears of future attacks, have been very deliberately exploited by the more repressive and violent elements in US politics to justify their preferred policies and agendas; and their pressure is influencing decisions in allied countries like New Zealand. Those who believe we must defend civil rights and democracy by suspending them are in ascendancy in the US, including increasing surveillance, restricting the movement of people and undermining legal due process.

(Earlier this month New York Congressman Jose E. Serrano said: "I fear some officials are so intent on fighting terror that they forget what we are fighting for. People across the spectrum fear for our civil liberties.") Amplified by irresponsible news media exaggeration of threats, this is creating a situation in New Zealand where serious ongoing erosion of civil liberties is possible.

It is clear that terrorism fears in the US serve a political purpose. New terrorism warnings are issued regularly, at times looking distinctly like well timed tactics to bolster political or public support for government actions.

New Zealand is further from the threats and so less prone to hysteria. But there has still been a pattern of over-reaction to supposed terrorist threats. After US hysteria about anthrax in letters (based on a single incident), we had weeks of anthrax scares – with scary pictures of people in white suits and sealed off mail rooms. Instead of playing down the obviously minimal risk, the dramatic publicity encouraged a series of deliberate scares.

Then came the cyanide threat in a letter to the US embassy at the time of the New Zealand Open golf tournament in January last year. Although it looked like an attention-seeking stunt rather than a real threat, the Police obviously could not just ignore it. However, in my opinion, they over-reacted badly. Someone seriously planning mass murder at the Golf Open would hardly have announced it in advance. But the Police ordered lots of staff back from their Christmas holidays and mounted a large operation.

The Police investigation included interviewing a Hutt Valley man about his possible links to the threat. What had he done to go onto the suspect list for these threatened murders? He had written an ordinary anti-war letter to the newspaper and – take note of the refined police intelligence at work here – he had an Arabic-sounding name. During the Golf Open armed police officers surrounded a man on the hills south of Paekakariki – far from the golf course – and took him to be questioned at the Porirua Police Station. He was a conservation worker who had been using a 22 rifle to shoot native bird predators in the nature reserve land in which he was working.

In fairness to the Police involved, these incidents were only months after September 11 and they were scrabbling around to deal with the situation. But, when more than a year later the (probably same) person again tried to get attention by sending cyanide threats, the Police reaction was again surprising. The original January 2002 letter had been leaked to the media, so could not be kept quiet. But when a third such letter was sent earlier this month (March 2003), it was the Police themselves who decided to publicise it.

The newspaper billboards in Wellington (on 11 March 2003) read "TERROR THREAT – CAPITAL NAMED AS TARGET". The news stories reported threats of putting cyanide in tap water, using explosives and gassing a cinema. Police publicised an 0800-THREAT telephone number and named noon 28 March 2003 as the threatened date for a "demonstration of capability". You would think that al Qaida were arriving en masse in New Zealand.

In my opinion, the news media acted foolishly, revelling in the sensationalism. The *Dominion Post* beat up the story to the maximum, exploring every possible angle of public

threat. For instance, a large story titled "Cyanide, what to watch for" informed readers that "when eaten" cyanide "may cause a bitter, burning taste, and/or numbness and tightness in the throat…. Breath smells of bitter almonds." This ridiculous stuff is ratings-driven journalism, like the preoccupation with dangerous dogs, killer bugs, home invasions and other thrilling fear-creating news stories. The news editors obviously took no responsibility for the fact that the disproportionate publicity given to one letter richly rewarded the letter writer and encouraged others to do the same.

In another article ("Stock up on water, public told") Wellington Mayor Kerry Prendergast advised the public to store water. Never mind that buried in another story the regional water managers explained that the threats were not realistic, it taking very large quantities of cyanide to produce dangerous levels in the water system. The Wellington City Council chief executive Garry Poole told the *Dominion Post* that the risk of water contamination was "very unlikely". More sensible headlines would have said something like "'Unrealistic' threat seeks anti-war publicity".

If that is what those responsible for the water supplies believed, why did the Police even announce the letter? Why would they create public concern that was probably unnecessary and give the letter writer exactly the publicity he or she sought?

The new police, assistant commissioner Jon White, said that Police had to warn the public because they believed the letter writer could be the same person who made the threats during the Golf Open. "There is enough there to think that we are dealing with something that has extended now over 14 months. There is certainly a sustained pattern of conduct."

If two previous letters constitute a sustained pattern of conduct, then the pattern revealed was of grandiose threats that had turned out to be nothing. The real sustained pattern in New Zealand is that we do not have serious acts of political violence. Of course the Police and other authorities should be watchful in case this changes, but publicising the cyanide letters seems like a gross over-reaction.

I have been told by Police that the standard practice for handling all manner of anonymous threats is to look into them quietly but not to give those making the threats the attention and reaction they are probably seeking. The aim is to avoid copycat stunts, minimise recurrence of the threats and minimise the stress and disruption caused by what are most likely empty threats.

Why didn't the Police follow their own procedures in this case? There may be some good reason I do not know about. But it feels like an unhealthy combination of over-reaction and vested interest. The vested interest part relates to the way that fears of terrorist threats are helping various government agencies gain new powers, resources and staff and strengthening their linkages to their preferred US and British partners – extra powers, resources and linkages they would always have liked but could not previously justify.

Heightened fears of terrorism in New Zealand are being used to justify all sorts of new Police and intelligence agency powers. The Counter-Terrorism Bill slipped into Parliament just before Christmas last year, for instance, includes serious changes to the balance between civil liberties and state surveillance and investigation powers. The bill seeks to

remove the long-term safeguard of not allowing information gathered under a search warrant for one charge to be used for another charge. The obvious purpose of this safeguard is to stop Police using contrived excuses like drug investigations to do investigative fishing trips. The bill proposes allowing use of "fortuitously" gathered evidence for any charges, not just terrorist ones – an invitation to abuse search powers. Among numerous other provisions, the bill also allows the use of electronic tracking devices and new powers to require individuals to hand over computer encryption keys to the Police to assist surveillance of their communications and computer files.

This latter provision was originally proposed (following similar proposals in Britain) in about 2000 – before September 11. Justice officials and later the Law Commission both argued against it, saying that forcing people to hand over their own encryption keys clashed with the traditional right of suspects not to have to incriminate themselves. The idea was dropped. Yet by late 2002 the provision was back, now as part of counter-terrorism legislation with the full weight of the terrorism hype behind it. It is likely to be passed this year.

When major new powers like this are proposed, justified by terrorism, my reply is: "where are the dead bodies?" If New Zealand had suffered a succession of car bombings, or if there were known groups with terrorist plans or links in the country, or if there were serious risks of foreign terrorists arriving here, then maybe draconian changes such as these could be justified. But actually all we have is exaggerated, sweeping claims and news media beat ups about theoretical future threats.

Privately, government officials have advised the Government that they believe the threat of terrorism in New Zealand is low. The advice is that there is no evidence of terrorist groups in New Zealand or of links between overseas terrorist groups and New Zealand. This sort of advice suggests that a careful watching brief should be kept, but that there is no need to reduce civil liberties. Yet that is what is happening.

On top of the new powers, heightened terrorist fears are also helping the police get extra resources and staff. For instance, the assistant police commissioner Jon White who publicised the cyanide letter this month had recently been appointed to a new position in charge of counter-terrorism and domestic security. There is a new 12-person Strategic Intelligence Unit based in the Office of the Commissioner at Police Headquarters. Originally set up temporarily after September 11, the unit has now got permanent funding and will be reponsible for intelligence collecting and investigations focussed on terrorism and international crime. There are now police liaison officers in Washington and London to increase co-operation in intelligence gathering and responses to terrorism with those two countries. And there are plans for the para-military Special Tactics Group to become full time because of the supposed increase in threats. These new positions and expanded structures serve to create a vested interest – a bureacratic and personal stake – in maintaining public and political concern about terrorist threats.

The counter-terrorist expansion occurring in the Security Intelligence Service is particularly telling. The SIS spent much of the 1990s floundering around trying to justify its existence in the post-Cold War world. After decades of monitoring the Soviet Union, China, all other eastern european countries and New Zealanders in left wing groups, it had

been trying out new roles like "economic security" to maintain itself. Now terrorism – which means helping its traditional allies fight the so-called war on terrorism like it earlier helped them fight the Cold War – has been embraced as the new raison d'etre.

In January 2002 the Government gave New Zealand's intelligence agencies an extra $5 million per year of operating costs for "counter terrorism efforts" plus $900,000 in new capital expenditure for the SIS. All details were kept secret. It is disturbing to find what "counter-terrorism efforts" mean for the SIS.

I have heard that the extra SIS spending is going to expanding the SIS surveillence and intelligence staff, particularly in the SIS's Auckland regional office (overall a 40% rise in SIS staff numbers will occur over about three years). The $900,000 is for new surveillance equipment, including a new, high-tech surveillance vehicle.

Significantly, the funding also provided for a new SIS liaison officer now located in the New Zealand embassy in Washington. His or her job will be co-ordinating New Zealand's assistance to Bush's war on terror and being a conduit back to Wellington for US intelligence priorities and concerns.

So who is the target of this expanded SIS "counter-terrorism" surveillance? The horribly predictable answer is New Zealand Muslim people. That is specifically whom the money was approved for. The increased Auckland surveillance and the new surveillance equipment are primarily to spy on mosques and New Zealanders who happen to be Muslim in the Auckland region.

They would not admit it publicly, but the SIS and other New Zealand agencies are following the FBI and other US agencies in equating terrorism with people of Middle Eastern and Muslim descent. For instance, shortly after the September 11 attacks, all major airports in New Zealand received a list containing the names of many hundreds of suspected terrrorists to watch for if they tried to board aircraft. According to airline people who saw the lists, every one of the 60 pages of names was Arabic. The lists came from the United States.

Our foreign intelligence agency, the GCSB, will similarly be using its resources to help track terrorism as defined by its US and British partners. Helen Clark has publicly stated that GCSB assistance is being made fully available for the US war on terrorism.

The Bush Administration's war on terror is not anti-terrorism per se – only anti-terrorism as defined by that Government's view of its friends and enemies. Despite claims to the contrary, the terrorist threat New Zealand has agreed to help fight (more to protect a western flank than specifically to protect New Zealand) has an Arab face.

If this suspicion was being directed at all Jewish people, or all blacks, it would be clearer to many people how obscene this targeting is. Why not monitor synagogues and freeze funds being sent to Israeli Zionists involved in political violence? It is very clear that the policies being pursued are taking sides in the United States' Middle East agendas, not countering terrorism. If someone supports US-sponsored terrorism in Baghdad or Israeli-sponsored violence in Gaza, no one will monitor them in New Zealand.

The irony of this approach is that the main way that New Zealand could become a terrorist target would be through needlessly taking sides in the Bush Administration's plans. In the unlikely event that a Bali-type bomb ever goes off in New Zealand, I will personally hold government officials and certain Ministers responsible because of the unthinking pro-American bias in their actions. The new "counter-terrorism" surveillance, and the alliances that prompt and underpin it, may be not only harming civil liberties in New Zealand but undermining the country's security too.

We have seen this all before, during the Cold War. At that time, New Zealand's alliance loyalties led it to get caught up in seeing the whole of Eastern Europe and many other countries as threats. Ordinary people from countries like Czechoslovakia and East Germany lived with low-level suspicion wherever they travelled. I know this from first hand experience, after a US Wellington embassy report in the 1980s apparently raised the possibility of spy links between me and my Hungarian homeland. The secret report did me no harm, but it could have if I had been trying to gain entry to this country at the time. (The joke was that I do not happen to have any family links with Hungary.) Now we have just swapped eastern european for arabic features in our "how to spot the enemy" kits.

In the erosion of civil rights that is underway, it is Muslim and Arabic New Zealanders whose rights are most at risk. They need the support of other New Zealanders at this time. Their targeting by state agencies follows the similar treatment of Muslim and Arabic Americans. Earlier this month Ibrahim Hooper, of the Council for Islamic American Relations, told the *New York Times* that "All Muslims are now suspects. We have to assume that every mosque in America is being bugged by the FBI." (16 March 2003).

My view is that New Zealand faces a minimal risk from terrorism and that joining the US war on terrorism will only increase the risk. It is the same lesson the country slowly learned during the Cold War: that detaching from the nuclear arms race was much safer for New Zealand than taking sides in it. Our best hope, when faced with fundamentalism to the east and west, is to give priority to maintaining a free and democratic society where no groups of citizens have to fear the security services. The rapid loss of privacy and civil liberties in the US and allied countries – under the influence of the current extreme US administration – should not be the standard for this country.

The alternative is for terrorist threats to be discussed openly and realistically, and for decisions on "counter-terrorism" to be more broadly based than just the secret advice from officials in closely US-aligned police and intelligence agencies. One outcome should be a major review of privacy and civil liberties in New Zealand – responding to the dramatic technological changes in surveillance capabilities – leading to a comprehensive new privacy law and updating of other civil liberties legislation.