WORLD BAR CONFERENCE 2014
Queenstown, New Zealand

Session 10: Surveillance versus privacy: the balance between the State, the Fourth Estate, the citizen and the rule of law

Julian Miles QC

New Zealand

WORLD BAR CONFERENCE 2014
Queenstown, New Zealand

SURVELLIANCE VERSUS PRIVACY: THE BALANCE BETWEEN THE STATE, THE FOURTH ESTATE, THE CITIZEN AND THE RULE OF LAW

BY JULIAN MILES QC

The view from New Zealand

Five years ago it would have been improbable that this topic would be the subject of a serious session organised by the NZ Bar Association. While most of us have been aware of New Zealand's involvement in the Five Eyes surveillance program together with Australia, UK, Canada and the USA, most of us were prepared to accept the official assurances that it was international terrorism and criminality that was being spied on. Again while it was common knowledge that electronic data from mobile phones and computers was vulnerable to hacking, few of us would have believed that Government agencies would be involved in systemic illegal spying on New Zealand citizens or that there was a real likelihood that the Five Eyes surveillance program would involve the gathering and distributing of private and personal information on New Zealand citizens.

Those relatively innocent days were changed with the Snowden revelations in 2012 closely followed by the Dotcom fiasco in New Zealand in late 2012.

Dotcom was a German multi-millionaire who had permanent residence in New Zealand. He was also the prime mover in Megaupload which had come to the notice of the Hollywood movie industry as being one of the largest file hosting websites in the world. At its peak it was said to be the 13th most visited site ever on the internet. Hollywood, backed by the Obama administration, considered such sites were designed to facilitate massive and systemic breaches of copyright. As a consequence the American Department of Justice, acting on those complaints, sought the assistance of the New Zealand police and the Government Communications Security Bureau (GCSB).

The charges laid by the American authorities were essentially for copyright infringement but backed by allegations of money laundering and racketeering. Their strategy was to obtain the appropriate search and seizure warrants in New Zealand, raid the Dotcom mansion, seize as much evidence as possible from Dotcom's electronic systems and apply for extradition to the USA.

The Americans were given enthusiastic support by the New Zealand authorities. To an extent unprecedented in New Zealand 76 New Zealand police officers, some equipped with machine guns and arriving by helicopter, raided the mansion. Dotcom and his three other associates were arrested at gunpoint and jailed. 135 electronic items were seized containing 150 terabytes of data. His assets including bank accounts were frozen and bail was denied for some months. Megaupload was closed own.

Dotcom responded by challenging the legitimacy of the warrants. During the extended court proceedings it became clear that the GCSB had spied on Dotcom and his associates for some months by accessing phone, email and computing records. Extraordinarily the whole exercise was illegal as the Government Communications Security Bureau Act 2003 forbad the electronic spying on New Zealand citizens or those who had permanent residence in New Zealand. Despite Dotcom's status as a permanent resident being well known to the relevant Government departments it appears this was overlooked by the GCSB.

The Government's response was to commission an extensive enquiry into the governance of the Bureau. The Report[1] identified a disturbing pattern of non-compliance with its statutory obligations. These included an institutional belief, totally unfounded, that the Bureau could lawfully obtain and provide information relating to metadata belonging to New Zealand citizens without the authority of a warrant. It appeared to be on the understanding that metadata was not a "private communication" for the purpose of the prohibition expressed in section 14 of the Act. Hence if the GCSB was asked by the SIS or the police to intercept New Zealanders' telephone records, emails and internet behaviour then it was free to do so.

The investigation disclosed 85 examples of such illegal spying on New Zealanders since 2003. One of the more alarming aspects of the review was the fact that not once during those 10 years was the illegal activity of the Bureau picked up by the Inspector General of Intelligence and Security whose role included the oversight of the GCSB's activities.

The review and the widespread concern at the illegal spying on Dotcom and the revelation that this had been the practice of the GCSB for at least 10 years led to an amendment of the Act.[2] The primary effect of the amendment was to legitimise spying on New Zealanders so long as an interception warrant or access authorisation is granted by the Minister. The grounds on which such warrants or authorisation can be granted are defined in wide and very general terms. It seems unlikely that any such application would be refused. Spying on foreigners appears to be permitted without warrants.

The amendment has been criticized as expanding the circumstances which would permit extensive surveillance of New Zealanders. In part this results from increased powers under the Act and in part arising from New Zealand's involvement in the Five Eyes surveillance program. Documents that came to light from Snowden and the Dotcom litigation indicate that the Five Eyes members share most of their surveillance activities. It also seems probable that New Zealand, through its Five Eyes connection, has access to certain of the US surveillance systems, including Prism, which the US has used to obtain metadata from Facebook, Gmail, Google and other social media.

Papers released from the Dotcom litigation show mobile phone numbers, email addresses, IP addresses of Dotcom and his fellow defendants were not only obtained illegally but were sent to US intelligence authorities.

The problem is that so many more transactions are now handled electronically that a much larger proportion of one's personal life is now being recorded and stored electronically – banking transactions, internet browsing, driving habits, cell phone location and activity, and emailing patterns.

---

[1] Review of Compliance at the Government Communications Security Bureau by Rebecca Kitteridge published on March 2013.

[2] Government and Communications Security Bureau Amendment Act 2013.

As more transactions have become digitalised the Government has acquired an almost unlimited capacity to gather, store, analyse and sift through electronic data.

But even under the new regime the GCSB continues to make serious errors. In a report issued under the new oversight regime for intelligence agencies the Inspector General, a former High Court judge, Andrew McGechan noted that the GCSB had tabled the wrong information on intercept orders in its annual report to Parliament last year. Instead of reporting the number of legal authorisations the agency had obtained it reported the number of operations it was conducting. The Inspector General noted it was "a severe experience for the GCSB but could not explain the error due to security risks". The problem, it was said, occurred as a consequence of the Bureau not understanding how to properly record its interception applications. The report noted that there needed to be some systems in place to "provide sufficient safeguards".

Coincidently at the same time as the Dotcom controversy was emerging a further and particularly chilling example took place of blatant breaches of journalistic confidentiality and privacy by the Government. The issue arose out of a story published by Andrea Vance based on a leak of a confidential report from a Ministerial office. She was a journalist based in the Press Gallery in Parliament. She refused to name her source. An inquiry was immediately ordered by the Government to track down the source of the leak with the suspicion being that the report had been leaked by one of the Ministers involved. The Government wanted to know what involvement the journalist had had with the Minister at the relevant time.

As a consequence Parliamentary Services, the organisation set up to run and administer Parliament was pressured by the Government to hand over all the electronic data monitored by Parliamentary Services including the journalist's emails, phone records and swipe card records. The metadata released to the inquiry included a 3 month log of calls she had made to people around Parliament. It would have included the phone numbers, the time and dates of the phone calls. Obviously the intention was to track the source of the leak. The inquiry had no powers to require this information and Parliamentary Services had no mandate to deliver it. Nevertheless under Government pressure all of the electronic information sought was handed over.

As a consequence there was an immediate investigation by the Privileges Committee which was highly critical of the investigation and the decision by Parliamentary Services to hand over that information. It was regarded as being a significant overreaching of any legitimate powers that the inquiry had. It was particularly objectionable on the basis that no consideration had been given to the special status of both MPs and journalists.

If there was any upside to the contempt shown by the executive to the long established right of journalists to protect their sources then it was the response of the Privileges Committee. However if one was being sceptical it seems possible that the primary driver for the subsequent inquiry by the Committee and the resulting criticism of Parliamentary Services was that members of Parliament were being investigated in this way rather than journalists.

If the experience of Andrea Vance, a senior journalist operating from the Parliamentary press bureau, is indicative of the ease with which basic journalistic rights and expectations can be overturned then the future is depressing.

Ironically the leaked report was a very detailed report prepared by Cabinet Secretary Rebecca Kitteridge on the governance of the GCSB. It was that report that found that the GCSB had illegally spied on as many as 85 New Zealanders.

It is clear that journalists are now working in a different environment than was present before 9/11. Government agencies including the SIS are now entitled to seek assistance from the GCSB to intercept phones, emails, social networks etc. The expanded powers of the GCSB, the practice of the Five Eyes in sharing intelligence and the examples of illegal activity by the GCSB and the Parliamentary Services in New Zealand inevitably has and will continue to have an effect on the way journalists in New Zealand practice their craft.

The clearest manifestation of this is the increasing difficulty that journalists are facing in being able to persuade contacts to provide information essential to the role of the journalist. If the promise to maintain anonymity for a whistle blower is perceived as being hollow through the ability of Government agencies to intercept the journalists' electronic records then the sources dry up.

New Zealand has always recognised the importance of whistle blowers to our society. There has been a long history of men and women who have risked losing jobs, friends and even family as a result of leaking stories of institutionalised fraud or wrong doing.

Traditionally journalists were given some protection by the common law when they were challenged to name their sources. These protections are now enshrined in s68 of the Evidence Act 2006. Specifically the Act grants journalists working for news mediums protection from naming their sources when the information is provided in the expectation that the information may be published in a news medium. However as one would anticipate there is also a discretion allowing the Court to overrule that entitlement when the public interest in disclosing the identity of the informant outweighs any likely adverse effect of the disclosure on the informant and the ability of the news media to access sources of facts.

The acknowledgement of the importance of the obtaining and disseminating of information to the public is underpinned by the right of the public to this information. See s 14 of the Bill of Rights Act.

New Zealand, unlike the UK, has also recognised the tort of privacy and the importance of that right to all members of the public including journalists.

These statutory and common law protections have had a mixed response in the Courts.

In *Police v John Campbell* [2010] 1 NZLR 483 John Campbell of TV 3 was ordered to name his source who had admitted to a high profile robbery during an anonymous interview with Campbell. The Judge accepted the police argument that the evidence against the source was thin and the admissions made during the interview were likely to be the primary evidence that would convict the defendant. Randerson J considered the public interest in ensuring that criminals are brought to justice overrode the right to anonymity and that the journalist could not have expected his promise to have been effective.

More recently in litigation still before the Courts the District Court declined to extend this protection to bloggers. His Honour argued that blogging was not journalism and hence the defendant, a well-known blogger under the name of Whale Oil, had to reveal his sources. In the High Court this ruling was challenged on the basis that the definitions were deliberately widened by Parliament to include more recent forms of journalism including blogs.

The judgment has yet to be delivered but I think it is likely that the District Court ruling will be overturned and the protection extended to include journalists who are involved in blogging. Whale

Oil is a controversial figure but there was extensive evidence of Whale Oil disseminating and even breaking news stories.

A more interesting question will be how the Court exercises its discretion and whether it will override the privilege or not. At the time of writing this paper the judgment has yet to be delivered.

A more conservative view was taken by Winkelmann J in yet another spin-off in the Dotcom litigation. An experienced investigative journalist David Fisher, employed by the NZ Herald, wrote an unauthorised biography of Dotcom with the subtitle "*Spies Lies and the War for the Internet".*

The police sought discovery against Dotcom seeking documents held by David Fisher given to him as background for the book. Her Honour held that the protection for journalists under the Privacy Act, which has a similar definition of news activity as the Evidence Act did not cover books. Her Honour stated at para 70:[3]

"*The definition of news activity protects two different forms of journalistic endeavour in its two limbs: preparing stories and disseminating stories. The first limb protects gathering, preparing, compiling, and making of observations on news, for the purpose of dissemination. The second limb protects the dissemination of the prepared story, provided it is about news, observations on news or current affairs. The end product of the two activities is specifically provided for in the definition: Articles and programs. Investigative journalism takes its form in long, detailed articles, which are covered by the Act's definition. Books, however, are not."*

I think the judgment could have gone either way. The conceptual distinction between long and detailed articles covering current affairs and a book covering the same topic seems a fine one. The protections recognised by Parliament for investigative journalists would seem to be as, or possibly more, necessary to journalists when writing a book on the topic than if they restricted the disclosures to an article.

Against this background is there a likelihood that investigative journalists will find it harder to persuade contacts to come forward and are they likely to be increasingly wary about protecting their own confidential documents stored electronically. This has certainly been the case in the USA as evidenced by a remarkable review recently published by the American Civil Liberties Union and entitled *"With Liberty to Monitor All – How large scale US surveillance is harming journalism, law and American Democracy".*

The report published in July 2014 is a detailed assessment of how the mass surveillance undertaken by the US Government of US citizens has impacted on journalism and lawyers in that country.

The report records wide scale surveillance programmes, much of it illegal, run by the Government including the large scale collection of:

- Metadata related to domestic phone calls;
- The actual content of Americans' international chats, emails and voice calls;
- Business records relating to international money transfers;
- Massive amounts of cell phone location data;
- A since discontinued program to track Americans' internet usage and emailing patterns;
- Address books and contact lists from personal email and chat accounts around the world;

[3] *Dotcom v Attorney General* CIV [2014] NZHC 1343 para 70

- Sharing information among different agencies and with other Governments.

The *Snowden* revelation shocked journalists and potential sources. A consistent response from journalists was that surveillance had made sources much more fearful of talking. The *Snowden* revelations have "*brought home a sense of the staggering power of the Government". "I think many sources assume I am spied on. I am not sure they are right but I can't do anything about that presumption"* and many others along the same line.

One consequence has been a change in journalistic practices. Many journalists are now modifying their practices by using forms of encryption software, burner phones, and a decreasing reliance on digital technology involving US – based online service providers. All of this adds significantly to the time, expense and frustration with dealing with actual or potential sources. However by far the greatest impact has been the drying up of the potential sources, particularly those working for Government agencies.

This has been a direct result of the Snowden revelations and the increasing tendency under the Obama administration to prosecute Government employees who have leaked information to the media. No Government can tolerate egregious breaches of security but the combination of the factors noted above is having a corrosive effect on the day to day relationship between Government and journalists.

As the scope of surveillance increases and the information overreach by the Government becomes the norm the distinction between information that should be kept secure in the interests of the State and information which discloses illegal, criminal or unethical conduct by the Government becomes harder to discern. It also inevitably has the effect of hindering the free flow of information about Government activities that the public has a right to know about.

A particularly disturbing development in the US is the link that the Government is making with journalists publishing classified information as being analogous to theft. Greenwald, for instance, was likened to a thief on the basis of "selling his access to information for personal gain". This level of rhetoric aimed at journalists doing the job that investigative journalists traditionally do can only be designed to warn them off from embarrassing the Government.

While the impact of surveillance on lawyers is not strictly within the boundaries of this paper it should be noted that this report also recorded an increased concern by lawyers at the scale of electronic surveillance by the US Government.

Lawyers acting in litigation against the Government are particularly concerned at this development. Obviously it is of particular concern to lawyers acting in criminal cases, and in particularly terrorist cases in the US. However an intriguing and alarming example of how the Five Eyes are sharing information arising out of their surveillance regimes came to light in February 2014. Documents revealed that the communications of a US based law firm acting for the government of Indonesia came under surveillance by the Australian intelligence agency which in turn provided that intelligence to the US.

If this incident is simply the tip of an iceberg then it gives rise to serious concerns. It suggests systemic sharing of intelligence between the Five Eyes group of privileged and confidential information which would be illegal to provide if it was provided locally. Intercepting privileged material is specifically banned in New Zealand as it is in the US. However if the Five Eyes intelligence agencies are regularly circumventing this legal restriction by supplying the intelligence to other members which could not

legally obtain the information themselves then this is a very worrying concern for lawyers in each of those jurisdictions. The reality is that this concern has already impacted on the way lawyers are practicing in the US and their relationship with their clients.

Essentially there are three rights which are part of the fabric of a democratic society which are threatened by the current surveillance regime: “The right of Government officials to share information through the press with the public; the right of journalists to acquire and share information about the operations of Government; and the right of the public to access that information through the media.

Whether those rights are threatened in New Zealand to the extent they appear to be threatened in the US is uncertain at this stage. However New Zealand is a member of the Five Eyes, and is subject to the same national and international pressures as other countries. The recent disclosures of illegal activity by the GCSB and the deliberate extensions of its power to spy on New Zealand citizens suggests these rights are at least under threat.

At the heart of the problem lies the difficulty of balancing the legitimate right of the state to protect its citizens from terrorist acts and the means by which it achieves this object. Fighting terrorism in all its forms requires the most sophisticated use of surveillance techniques available to a government. This becomes a problem only when the state overreaches these powers so that it threatens fundamental rights of the citizen which the state is attempting to protect. This threat has become more insidious as intelligence agencies have acquired almost unlimited powers in the gathering and analysing of private data belonging to their citizens and the nationals of other countries.

The ability of the current US systems to hoover up private information acquired from the networks is staggering. In one thirty day period the NSA collected 97 billion emails and 124 billion phone calls from around the world. Documents published by Snowden indicate that the American intelligence agencies continue to seek more data rather than less. There is no reason to believe that this aim is any different to any of the other members of the Five Eyes. There are clear indications that the aim of proportionality between information acquired between protecting the state and protecting the rights of individuals is seriously out of kilter. The legal requirement of minimalisation appears to have been all but abandoned.

One consequence of this extraordinary increase in surveillance has been to limit the traditional role of the investigative journalist. A key component of that craft has been the legitimate expectation by the whistle-blower that their identity will be kept confidential. That expectation has already been eroded by the current surveillance regimes in New Zealand. Only time will tell what effect these current regimes will have on the ability of journalists to do their job. But the odds would appear to be stacked against them.