Sword or shield? The role of a Regulator

Paper by Mark Hummerston, Assistant Privacy Commissioner

Office of the Privacy Commissioner

Presented at

Interpreting Privacy Principles

Symposium

3 July 2007

Sword or shield? The role of a Regulator (Slide 1)

Oh, to be a Regulator last century!

Regulators had it easy then. Everything was black and white, and in some jurisdictions the regulator was virtually all-powerful. (Slide 2)

Take for example the Committee for State Security – the KGB of the former USSR. The KGB was the umbrella organisation for the Soviet Union's premier security agency, its secret police and its intelligence agency, and operated from 1954 to 1991. (Slide 3)

I should add, for balance, that in general terms the KGB's operational domain encompassed functions and powers akin to those exercised by the United States' Central Intelligence Agency (CIA), the counter-intelligence (internal security) division of the Federal Bureau of Investigation (FBI), the National Security Agency, the Federal Protective Service, and the Secret Service in the United States, or by the twin organisations MI5 and MI6 (the Secret Intelligence Service) in the United Kingdom.

Of course there were certain disadvantages to having such a powerful regulator in place. As a regulator the KGB operated almost without oversight, except by the "inner sanctum" of its political masters. No overlapping jurisdictional "turf wars", no political interference, no oversight agencies, no complaints, no appeals. The KGB did not have complainants – or if it did – they were mostly silent or incarcerated.

The KGB's terms of reference were simple. Sword and shield. Defend the revolution, smite the revolution's foes. Black and white. You were on-side, or you were off-side.

It is probably fair to describe the KGB as a heavy-handed regulator.

In contrast, it is equally fair to describe the Office of the Privacy Commissioner as a light-touch regulator. In general terms Australian regulators operate to encourage compliance and work cooperatively with the organisations and agencies they regulate. Coercion is a less used weapon in the armory.

So how do complainants, respondents and advocates see such light-touch regulators? My quick survey revealed:

(Slides 4, 5 & 6)

Complainants – "A knight in shining armour" – defending complainants? (Slide 7)

Respondents – "Child-eating ogres" – smiting respondents?

Advocates – "A toasted marshmallow" – neither sword nor shield?

It is true that there are different perceptions and expectations of regulators. A large part of the regulator's role is finding the balance between competing demands. (Slide 8)

A simple example illustrates my point. Consider the differing approaches to the issue of privacy notices:

Layered or staged provision of notice (Slide 9)

The tension between what consumers might want and what advocates might prefer is well illustrated when considering the matter of notice. The Cyberspace Law and Policy Centre described it in this way in its submission to the Australian Law Reform Commission's *Review of Privacy Issues Paper:*

"Privacy Commissioners around the world have increasingly been accepting, and even promoting, the concept of layered or staged provision of information. In August 2006, the Australian Privacy Commissioner launched a new presentation of her own office's privacy policy as an example of a 'layered notice' approach. The objective of such approaches is to avoid overloading individuals with too much information initially, but to retain easy options for them to find out more detail if interested.

Many consumer representative organisations, while acknowledging an 'information overload' problem view trends towards layered and short form privacy notices with suspicion, as they can too easily omit information which should be relevant to an individual's decision whether to proceed with a transaction. Discussion of this issue inevitably involved 'wider' political judgments about the extent to which legislators and regulators should 'force' information on consumers which they may well not generally welcome or make use of (e.g., because it is perceived as paternalistic and patronising)."

More information, or less?

Advocates suggest erring on the side of "more", so that consumers are fully informed about the transaction and its consequences. Consumers, confronted by reams of jargon-laden "fine print" want less – just the essential details.

The Office considered these conflicting desires, and formulated a layered notice format for its own privacy policy and as a model for other agencies and organisations to use as a template. At that time the Commissioner observed:

"Research has shown that individuals find privacy notices long and difficult to read and most do not read them at all. Layered notices are an effective means of communicating the personal information handling practices of an agency or organisation.

The Office's condensed Policy is easy to understand, using clear simple language and includes the most important information that individuals need and want to know about the Office's personal information handling practices.

Should individuals want further information the condensed notice enables individuals to easily link to the Office's full privacy policy, which addresses the Office's legal requirements.

I encourage agencies and organisations to consider adopting this approach to improve communications with customers and look forward to seeing layered privacy policies developed and implemented."

Balance

I use that example simply to illustrate the role this Regulator adopts. (Slide 10)

We operate in an environment – in a society – where "privacy" is not an absolute right. It is a right to be balanced with other interests – a good example is the public interest in openness and transparency in government administration.

The Privacy Act sets out *principles* to be applied, rather than prescriptive regulation. Applying principles, to be effective, requires balance and objectivity.

Indeed, the concept of "balance" was specifically referred to by the then Attorney-General, the Hon Lionel Bowen, when he gave the second reading speech for the *Privacy Bill 1988.* He observed:

"The enormous developments in technology for the processing of information are providing new and, in some respects, undesirable opportunities for the greater use of personal information. These developments have focussed attention on the need for the regulation of the collection and use of personal information by government agencies and for an independent community spokesperson for privacy. The Privacy Commissioner will ensure that some balance is brought to the debate as to the desirability of using the opportunities provided by new information technology to their fullest extent.

There is no doubt that with the greater range of services being provided, governments are accumulating more personal information about individuals in order to provide those services efficiently and effectively. This, together with the ever-increasing capacity of modern computers to search and process information, offers significant potential for invasion of personal privacy by misuse. Also, the legitimate needs of agencies in acquiring personal information and the use made of it must be balanced against the need to sustain personal privacy."

That is, there is a need to balance the often competing needs of the individual, the organisation and the public interest. As a regulator we seek to achieve that balance.

Proportionality

As an agency with finite resources – like every other agency and organisation – the Office has to choose how to allocate those finite resources to its various responsibilities.

As the Assistant Commissioner responsible for the Compliance function, I need to determine the best utilisation of resources to achieve the strategic goals of the organisation. What resource do I allocate to investigating complaints? How much time should be dedicated to conciliating matters? How many audits should Compliance undertake each year? What effort can I devote to uncovering systemic failures? How many "own motion" investigations can I pursue each year? (Slide 11)

The answer to each of those is, of course, that it is my responsibility to oversee the best utilisation of resources possible, resulting in effective and efficient complaint-handling and investigation. An over-concentration of resources on one activity will well mean that other equally important activities are overlooked.

As Ian Temby QC put it, as the first head of the ICAC:

"Choice of matters to be investigated depends upon several factors, particularly the nature and apparent cogency of information received, the workload of the Commission from time to time, and the need to have the activities of the Commission spread, but not too thinly. If too much is taken on then nothing will be done well. If all resources are devoted to a particular area, then corruption is likely to flourish elsewhere."

Let me take this a little further. My investigative staff – Compliance officers – all carry case loads of different matters. Let's say that allowing for administrative and other tasks, they have 30 hours per week to devote to case work – to investigations.

"Balance" might suggest that if they have a case load of 30 matters, each matter should be allocated an hour's worth of activity each week. No-one here I suspect would regard that as a sensible approach, even though we could say it was "balanced".

Clearly some matters are much more complex than others, and require more time to uncover the facts, let alone resolve the issue. Some matters will be more urgent than others – a failure to intervene in a timely way may increase the distress or disadvantage suffered by a party. Other matters are such that time may have less significance and little or no ongoing consequence.

For example, my credit card statement is posted to Nigel. I might be embarrassed that he knows the level of my indebtedness and I will be annoyed that my credit card purveyor made such a stupid mistake, but I also know Nigel is an honourable person. The mistake is hopefully a one-off incident and Nigel won't pass on the details to the *Daily Planet.* An apology, correction of the error and improvement of the enveloping system to prevent a recurrence will in most cases be sufficient. (Slide 12)

But when my credit card statement appears on say, the *Drudge Retort,* (not to be confused with the *Drudge Report*) I will be seeking an expeditious solution which includes ensuring the information on the website is removed

immediately! Nigel is honourable, but I can't be so certain about the thousands of people who may stumble upon that information on the web!

Proportionality is thus also an important touchstone for this Regulator.

One size doesn't fit all

I referred earlier to the KGB as a regulator. Largely that regulator applied the "one size fits all" solution to problems. (Slide 13)

My view is that a one dimensional approach by a regulator is fraught with difficulties, and destined to failure. There is no doubt that a multi-faceted approach to a issue – for us, privacy – is almost always required in order to bring about sustained change and improvement in behaviours, particularly organisational behaviours. Organisational culture is very hard to change – yet that is what often we seek to do in relation to promoting a respect for privacy within organisations.

Perhaps I can give a real-life example here.

First, a sense of déjà vu. Only yesterday I read in the *Sydney Morning Herald* the following: (Slide 14)

"NSW cop given $17,000 in bribes: court

July 2, 2007 – 1:14PM

A NSW police officer allegedly was paid more than $17,000 in bribes in a secret deal with a private investigator, a Sydney court was told.

Senior Constable Stephen Richard Evans, 48, is accused of giving Janice Seeto, 50, police information in exchange for payments of between $100 and $500 over a period of nearly three years.

Evans, who has been suspended from Green Valley police station, in Sydney's south-west, was paid a total of $17,900 between February 27, 2003 and November 11, 2006, Downing Centre Local Court was told.

Court documents show the time between payments ranged from less than one day to about three months. It did not show what information Evans was allegedly supplying Seeto with.

It was not revealed how investigators discovered the alleged scam, but the documents allege Seeto offered a bribe to a second officer between November 22 last year and January 12 this year.

Evans did not appear in court, where he was charged with 43 counts of receiving a bribe.

Seeto, who has been charged with 44 bribery offences, also did not appear in court on Monday.

The matter was adjourned to the same court on July 24."

For me this has a real sense of déjà vu. (Or at least the feeling that I have heard it all before.) And indeed I had. Back in 1991, when I first learned about the *Information Exchange Club.* (Slide 15)

The Information Exchange Club

"It is not only by illicit sale that the information has been disseminated and has been allowed to accumulate. Well-intentioned and sometimes authorised exchange of confidential information has also been a major contributor. That has occurred through the activities of what became known during the investigation as the Information Exchange Club.

Either by law or as a matter of practice, agencies involved in the investigation of crime have access to confidential information held by public authorities. There has also been co-operation among government departments and agencies in exchanging information for other purposes, including the recovery of debts.

The implementation of those arrangements over the years has been marked by considerable laxity.

Official department-to-department arrangements involving designated officers, were often replaced by unofficial arrangements between individual officers. Contacts were established at social functions organised for the purpose, apparently with departmental approval. Admission to the "Club" was extended to include people from banks and other financial institutions.

In consequence, an uncontrolled system of exchange of information developed, in which access to information depended on the unofficial private contacts a person had.

Unauthorised dissemination of confidential government information resulted. The Information Exchange Club became a source of information, both for those who sought it for what they regarded as legitimate purposes, and for others who wanted it for re-sale.

A person who was not a public official, but who had access to the Club through her previous employment in a private finance company, used it to obtain addresses of electricity consumers, for the sole purpose of selling them to a private investigator. Through the same means she developed a trade in confidential information from Telecom and the Department of Social Security. What she gave in exchange was information obtained by her in her employer's name from the Credit Reference Association of Australia, and improperly disclosed by her.

Another private investigator was able to use an employee of Sydney Electricity, whom he paid, to obtain information on overseas passenger movements. The Sydney Electricity employee in turn obtained the information through the Information Exchange Club, from persons employed in the Department of Immigration or the Australian Customs Service.

Officers of the Australian Customs Service traded New South Wales RTA information, to which they had direct computer access, for information from other sources.

A New South Wales police officer and an investigator employed by Telecom, exchanged information from their respective employers' records, and each sold what he obtained from the other to private investigators."

That summary came from what I knew as Operation Tamba – to most it was known as the ICAC's investigation and subsequent *Report on Unauthorised Release of Government Information.* Volume III of the report notes:

"A total of 155 persons were found to have engaged in corrupt conduct, and 101 persons found to have engaged in conduct liable to allow, encourage or cause the occurrence of corrupt conduct. Thirty-seven of those found to have engaged in corrupt conduct in connection with the trade in confidential government information were police officers at the time. Another eighteen found to have engaged in corrupt conduct in connection with that trade, were Department of Main Roads or Roads and Traffic Authority (RTA) officials at the time. All but one received corrupt payments for the unauthorised release of information. Known payments to RTA officials alone ran into several hundred thousand dollars."

The report also noted that the findings were the "tip of the iceberg". It would have been impossible to follow up every lead, to track down every public official, every individual, to trace every corrupt payment in that matter. The investigation sought to uncover corrupt practices and provide concrete examples – so that other solutions could be explored and implemented.

And perhaps yesterday's *SMH* article underlines there is still some way to go.

But the purpose of this example is to show that investigation (and perhaps even prosecution) is not necessarily a guarantee that changes in behaviour have been achieved.

A regulator cannot rely on investigation alone. The effective regulator has to adopt a range of techniques to bring about lasting change. Conciliation, education, prevention techniques, audits, guidelines, policy advice, investigations, determinations – all of these and more comprise the tool box of the modern-day regulator.

Fairness

As a regulator our approach must be guided by fairness. Generally speaking, individuals are disadvantaged when confronting an agency or an organisation – or making a complaint. An issue of importance to an individual may seem minor or of little consequence to a respondent. (Slide 16)

Our role is to bring balance – to help an individual and an agency or organisation focus on dealing with the issue of concern.

Fairness must go hand-in-hand with objectivity. The primary objective of the regulator, in carrying out an investigation, is to seek out the facts and establish the truth. The regulator's role is to discover the truth. (Slide 17)

That differs from what happens in courts of law. There justice is dispensed in accordance with the law. Courts decide matters on the basis of the evidence put before them – evidence chosen by the parties to place before the court. Judges are not charged with ascertaining exactly what happened – that is not their function.

We must deal in the objective facts and circumstances as they are discovered and then seek to apply that knowledge fairly, bearing in mind the relative positions of complainant and respondent. We must also bear in mind the public interest.

Looking forward

Investigations are essentially reactive. An event has occurred and a problem exists. Investigation can establish the facts, and the causes. Hopefully that particular problem can be resolved.

But investigation does not necessarily prevent that type of problem arising in the future. As my earlier example highlighted, the ICAC carried out an extensive investigation into the unauthorised release and sale of confidential information in 1990 – 91, yet as recently as yesterday we see an example of that illegal practice still occurring. (Slide 18)

As a regulator we must not only react to concerns, we must also be proactive – working with organisations and agencies to prevent or minimise problems occurring.

This means the role of the regulator is to "win the hearts and minds" of agencies and organisations about respecting and protecting privacy. (Slide 19)

To do that, we must approach privacy as part of the suite of good governance requirements. That requires building trust and earning cooperation. We need to help agencies and organisations bring about change in their systems, practices and culture. (Slide 20)

No longer can regulators afford to take only the "sword and shield" approach.

We are committed to defending privacy, and taking on those who disregard it. That will mean the occasional "smiting".

As a regulator we need to bring balance, proportionality and fairness to the protection of privacy. We do not live in a vacuum – there are competing interests. The right to privacy and the public interest. The demands of a complex society.

Good Regulators no longer have it easy!

Sources:

http://en.wikipedia.org

Cyberspace Law and Policy Centre – Submission to the Australian Law Reform Commission on the Review of Privacy Issues Paper (January 2007)

Office of the Privacy Commissioner – Layered Privacy Policy (August 2006)

Parliament of Australia – Hansard (November 1988)

Independent Commission Against Corruption – Annual Report 1989

Sydney Morning Herald – NSW cop given $17,000 in bribes (2 July 2007)

www.drudge.com (June 2007)

www.drudgereport.com (June 2007)

ICAC – Report on Unauthorised Release of Government Information – Vol. 1. (1992)