NZ Centre for Public Law
Public Office Holders' Lecture Series

"Constitutional Necessity or Constant Nuisance?"

The Privacy Commissioner and the Role of ICEs

Marie Shroff, Privacy Commissioner
28 January 2014

Introduction

This talk will be mainly about the constant tension between what is laid down in theory and what happens in practice with Independent Crown Entities.

I have always believed, in the constitutional context, that evolution is a better process than revolution, and has a more enduring outcome. The Privacy Act and the office were founded on some principles which have been tested by the process of evolution as the information age has advanced. In a living demonstration, we have seen over the last few years a test of the core principles of Privacy Act as well as those which underlie independent Crown entities. The Office of the Privacy Commissioner (OPC) continues to evolve before our very eyes. I believe this is a positive process, which requires constant re-examination of both principles and practice.

I should explain that henceforward in this paper I will refer to independent crown entities as ICEs; and Crown entities as CEs.

ICEs and Independence

Independence is the core value we stand for – without it we are useless as a democratic watchdog. At the start Bruce Slane, with the able assistance of his cartoonist son Chris, did not hesitate to throw a few "idea bombs" around, thus under-scoring the OPC's independence.

A recent academic article[1], by Carolyn Jackson of The University of New South Wales, examining the independence of Australian and NZ Privacy Commissioners, has come up with some interesting ideas about independence as an asset. She says "For regulators independence has become associated with good governance, reform and best practice. International organisations recommend it, agencies seek it, governments support it and citizens expect it." Her conclusions are in short that Commissions need to be "structurally separated from politicians and …to display qualities associated with independence such as impartial (not simply non-political) handling of complaints, trustworthy behaviour and public advocacy." Malcolm Crompton, former Australian Privacy Commissioner, also contributed strongly, at the end of his term in office, by proposing performance measures for ICEs, and privacy commissioners in particular. In summary he suggests the following measures:

[1] Jackson, C. 2014 (forthcoming), 'Structural and behavioural independence: mapping the meaning of agency independence at the field level', *International Review of Administrative Sciences* vol. 80, no. 2.

economic impact; social outcomes; public accountability for resources; independence, fairness, transparency and accountability in decision making; active engagement in policy making; ensure clear respect for law by all parties; and service provision.[2]

A little history. The Privacy Commissioner is what used to be called a quango. As long ago as 1984, the incoming Labour government called for a "Quango Hunt". Sir Geoffrey Palmer (then Geoffrey Palmer the politician) reminds us in his recent memoir that some people say quango stands, not for quasi-autonomous non-governmental organisation, but rather "quite unacceptable and nasty government offshoot".

There were indeed many and varied small semi government entities then - far too many for a small country. Successive attempts were rightly made to reduce the number; and this reductionism - combined with some nice scandals - eventually led to the passage of the Crown Entities Act 2004. The purpose of the Act is "to provide a consistent framework for the establishment, governance and operation of Crown entities … to clarify accountability … to provide for different categories … (to) clarify powers and duties … (and) to set out reporting and accountability requirements".[3] This managerialist approach was worthy in its place and time and the Crown Entities Act has performed usefully to standardise procedural aspects of Crown entity governance.

But policy thinking behind Crown entities or their reform has never been deep or wide. Tidy minded or mechanistic thinking, often driven by obsession with cost and little regard for value, has prevailed. Subsequent writing and analysis of the CE model is sparse. There is a 2009 article by D Gill, a troubling analysis from an official involved in the CE reforms. I quote "…the notion of Crown Entities that emerged as the result of accrual accounting……required the government to clarify which organisations it owned….Crown entity was essentially a residual category… a residual 'lump'. Justification cited for the Act included "avoiding special pleading" and the historical failings and scandals of CEs. The Gill paper's four fundamental governance propositions for Crown entities conclude with a chilling fourth proposition – "dealing with the shibboleth of independence involves balancing the inherent tension between being arms length and being a public body". Now I don't know about you but to me "shibboleth" means outdated sacred cow, or to quote the Concise Oxford: "catchword, especially old-fashioned and abandoned doctrine of a party or sect". (Whatever Gill's views might be now, the policy thinking, or lack of it, behind the Crown Entities Act, remains.)[4]

Independent Crown Entities in particular don't fit easily into the in-vogue model of outcome- and asset management driven public structures and of central control to ensure accountability. The Crown Entities Act attempted, as a principal goal, and in an understandable pursuit of efficiency and economy, to fit all Crown Entities into one administrative and governance structure. As a result, one thing ICEs now do not suffer from is a lack of formal monitoring and assessment. How successful that is, is quite another matter. Sometimes I think the endless Statements of Intent, Annual Reports, audit reports, Select Committee questionnaires and hearings are more likely to produce games of political paintball or repetitive sessions of political "gotcha", rather than a serious examination of the success or otherwise of particular ICEs. Bureaucratic (as opposed to political) monitoring of ICEs is often misguided and ineffective, probably because it is based on the defective analysis outlined above. Stephen Franks, in a 2009 address on Crown entity governance, remarked that "I see this conception of monitoring as a long term threat to the usefulness, to citizens and Ministers, of the Crown Entity structure at least equal to ... patronage

[2] Crompton, M. 2004, 'Light Touch' or 'Soft Touch'? – Reflections of a Regulator Implementing a New Privacy Regime. Speech to National Institute of Governance, Canberra; and Committee for Economic Development of Australia, Melbourne.
[3] Crown Entities Act 2004, s 3.
[4] Gill, D. 2009, 'Reform of Arms Length Government through the Crown Entities Act (2004), Institute of Policy Studies Working Paper 09/12.

appointments…" [5] The Crown Entities Act thus provides only a partial approach to how well ICEs fit within, or contribute to, a better New Zealand.

Media and bloggers i.e. 4th and 5th estate scrutiny, sadly, rarely extends beyond examination of six-monthly expense account returns to see how much was spent by CE heads on food or drink. It would be nice to think editors might instead invest some real resource into genuine analysis.

A New Approach to ICEs

I believe we need a new way. A first principles approach to ICEs should be that they are part of the fundamental equipment of a "high functioning" democracy; essential to hold government, business and civil society institutions to account. Consistent with my earlier writing from the Cabinet Office on MMP, Cabinet and democracy, I believe there is a need for robust checks and balances, to ensure public trust in government and business institutions especially in a country lacking a second chamber or an entrenched Bill of Rights Act. ICEs in particular are essential. They are part of the necessary "on board safety kit" for every well-equipped ship of state. What is lacking is some serious academic and policy scrutiny of ICES and perhaps Crown entities generally, to see how the model is working and how we can more effectively measure their value, in principle and practice, to ensure both democracy and value for money.

Characteristics of ICEs

What are the characteristics of ICEs against which it would make sense to hold us accountable to Parliament? I will have a first go at this, drawing on my own experience over the years and on the useful work of Jackson and Crompton.[6] I make no claims that my proposals are complete or anything more than a first attempt.

- **Independence** - with associated agency qualities of fairness, impartiality and transparency; and including ensuring independent appointees to statutory positions
- **Effectiveness** - including social and economic impact and credibility
- **Regulatory and enforcement credibility and mandate**
- **Service to clients**
- **Advocacy**

I propose this list as a start towards assessing the real value of ICEs to NZ: the current procedural monitoring process of the Crown Entities Act barely touches these aspects. A focus on success and impacts would assist both Parliament and the media to ask the right questions in assessing ICE and CE performance.

I note in passing, but as a significant point of context, that many of these characteristics will apply to a greater or lesser extent to CEs other than ICEs ie the less independent Crown entities - the autonomous Crown entities and Crown agents. Between us Crown Entities have 70% of government employees, 65% of fixed physical assets and 50% of spending on services to the public. ICEs are clearly at the small end of these large figures, and because of our independence, rightly at the outer rim of government control. One risk is that Crown entity governance will be driven by the resource intensive hospital boards and ACCs of this

[5] Franks, S. 2009, 'Governance in Boards of Crown Entities', Speech to 3rd annual conference on Legal Issues for Crown Entities, Wellington, 23 September 2009.
[6] Ibid 1.

world, distorting a clear view of appropriate governance for ICEs. Excessive tidy mindedness is not necessarily our friend.

A looming question is how resources to independent Crown entities are currently managed. A restricted diet is of course an effective way to weaken independent entities. The CE Act model for ICEs leaves them at the mercy of budget policy and without an effective voice in the highly competitive budget process. The public also needs to be confident of the independence and credibility of statutory appointments to Crown entities. (I am happy to say present company and my successor are excepted from questions on this score.)

And then there's law reform. I first saw a draft Cabinet proposal to make necessary amendments to the Privacy Act in 2004 just after I took up office. A Law Commission report, many more draft Cabinet papers, several governments and 10 long years later, reforms are yet to emerge. Again, I put this down partly to a lack of effective voice for CEs at the decision-making table.

These three issues, of funding, law reform and appointments, raise an interesting question as to whether ICEs should have more safeguards for their independence. For example should they all be parliamentary offices and therefore directly appointed, provisioned by, and accountable to a multi-partisan parliamentary committee? Successive governments also need to be held accountable for their handling of ICE's status – for the quality of monitoring, resourcing, law reform and appointments to their top positions. All of these would be great subjects for further examination – academics please get stuck in.

However, a note of warning here. Some years ago Canadian academic Dr Donald Savoie mounted a considerable assault on the multiple officers of parliament that exist in the Canadian setting (e.g. the Privacy Commissioner is an Officer of Parliament). This assault apparently did not have huge practical consequences but it is interesting to hear his contrary note. He said *inter alia* that "Officers of Parliament….get up in the morning thinking of ways to be relevant and visible… (and) ... it is difficult to ask bureaucrats, who tend to be risk averse in the first place, to take any risk when 14 officers of Parliament and their staffs – accountable to no-one except, perhaps, God – are looking over their shoulders every day." [7] My personal view is that credibility requires the numbers of ICEs to be kept to a necessary minimum, as well as improving their performance measurement. Perhaps too many Officers of Parliament may be the real driver of this Canadian discontent.

OPC and the Last 10 Years

I'd like to turn to the role of the Privacy Commissioner over the last decade, which provides an interesting case study of the evolution of an ICE in the rough seas of an economic recession, and in our case, the tsunami of technology. My account of the last 10 years will run wider than the ICE model to give you a picture of our turbulent decade.

For the last 10 years, from my office, with a view of the working part of the harbour in Wellington, I have seen little red tugs battling to get unwieldy large ships into a safe berth, often in gale force winds. The story of OPC in the last decade has been a bit like that of the little red tug and the ocean liners. As we move through that I ask you to bear in mind my list of ICE characteristics – independence, effectiveness, regulation, service and advocacy.

[7] http://www.theglobeandmail.com/report-on-business/rob-commentary/oops-ottawas-mistake-of-grand-proportions/article1366833/

Let's take a walk through that decade. What did OPC look like then?

- Classic legal office style and approach
- Starved of resources
- Large complaints backlog
- Policy and data matching struggling under huge work load
- No technology expertise
- Substantial track record already with health and telecoms codes, public education
- Public image probably equivocal, bedevilled by the BOTPA perception (Blame it on the Privacy Act)

Context and Players: Early 2000s

The reference book, the pen, the letter and the fax machine were still dominant, but fast giving way to email, social media and the search engine. 9/11 of course was a defining moment early in this century, which marks a turning point. Resulting laws pushed strongly towards mass government surveillance, placed a high value on security, and a low value on privacy. The internet and technology generally were on a rising curve but Facebook hadn't even been thought of and Google was in its infancy.

Privacy was unpopular with the media - Bruce Slane said in his final annual report that the media even referred to OPC as the "Gestapo" and the Commission as "Commissar" or "Tsar". He talked about the "lonely stand" OPC had to make on some issues. As recently as 2006, the Dominion Post made an editorial attack on privacy headlined "Creepy and Dangerous".

Most of you know about the concept of the classic regulatory pyramid with the wider base of the diagram made up of willing compliers and the narrower point of the triangle made up of reluctant compliers, or actual rogues. Early on, I would have to say that pyramid was almost inverted; reluctant compliers were numerous and at the base of the pyramid.

The public sector at that time was unconvinced of good information handling needs: many senior managers in departments and state sector agencies were openly dismissive of privacy and blind to the collateral damage to client trust, and to the efficiency and ethical issues. Large businesses were ahead of the public sector because many were applying good privacy standards from more sophisticated regimes from HQs overseas; the banks for example have always been leaders in this area and could see the direct relationship between good personal information handling, customer trust and a healthy bottom line.

Where was the public mind at this stage? In 2001 our polling showed public concern about privacy at a middling 49%; media driven concerns about freedom of speech, and fairly trivial, often inaccurately reported, stories about access to school reports and airline passenger information and the like influenced public attitudes.

In those early years, therefore, my main preoccupations at OPC were struggling to get the complaints backlog down; developing a code to control credit reporting; working on improving our public image by pointing out to the media that they were missing one of the main stories of the century by focusing on the Privacy Act as a block or impediment ("BOTPA"), rather than on the flood tide of technology and the surveillance society.

How were we as an ICE, against my tentative characteristics? In the early part of the decade this is a picture of an ICE struggling, and partly succeeding, to establish mandate, credibility, effectiveness and service. Our advocacy was strong but our internationally driven Privacy Act had yet to gain real traction in the NZ environment.

- **Independence** – probably reasonably good, but qualified because of the following points:

- **Effectiveness** (economic and social) – I'd have to say low to medium success, partly because lack of resources prevented us doing more than a very few regulatory initiatives e.g. the Telecoms Code, the Credit Reporting Code

- **Regulatory and enforcement credibility and mandate** – could do better – backlogs of complaints, few resources, and public perception of privacy as an obstruction were handicaps

- **Service to clients** – slowness on complaints and almost everything else (resources again) meant our reputation was fair because we clearly tried hard, but it was far from brilliant

- **Advocacy** – here I think we scored well – the media were hostile but we gave as good as we got, and constant repetition of our core messages began to serve us well.

The Journey to Now

I will now take you on a fast ride from the early 2000's to 2014.

Just to remind you of the pace and scale of the technology revolution: the rise and rise of Facebook and Google and Apple and Amazon and more; the appearance of data mining and big data analysis; cloud computing – it started with little fanfare but slowly became a buzz word of the times; the mega growth of computing power and storage; the gadgets which have almost taken over the world – Skype, smartphones, Paypal, mobile computing, location tracking, Google Glass, facial recognition, drones, Maxwell Smart wristwatches, the internet of things – it's all happening.

And let's recognise how these changes became rocket fuel for the growth of government and business databases, and silently handed over to them on a plate the power to collect, farm and exploit those vast data stores for business and government advantage – and of course to enhance consumer service. For just one example of growth, complexity and power in technology, look at the rise of 'the stack' – we are seeing an increased reliance on a handful of companies providing us with multiple services. Major internet corporates want to corral you into relying on their services alone.

This is a quote from an essay called 'Android is Better'[8] by a Twitter designer Paul Stamatiou:

- Most services I rely on daily are owned by Google. My world revolves around Gmail and Google search. I could start listing android features I adore, but this succinctly states why android makes sense for me; the number of Google products I use each day bothers my mind. No other company has imbedded itself this deeply into my life.

And government is no different – it recently passed an amendment to the Privacy Act that allows information about you and me to be widely used and shared across government. I welcome the privacy safeguards that have been built into this legislation, at the suggestion of my office and the Law Commission. But there is no getting away from the fact that there is also a government 'stack' developing, which will share our information and dominate much of our lives into the future. We are born, we use the health and education systems, we get married or live together, we pay taxes, we get a passport, we fill in census forms, we register a company, we get a traffic fine or break the law or go to prison, we receive a benefit, we

[8] http://paulstamatiou.com/android-is-better/

cross the border and come back, we get government subsidies, we retire and get superannuation. When we die that fact is digitally recorded but while we may be gone we are not digitally forgotten.

And let's not forget what we do willingly ourselves – we social network, we use cloud storage, we buy and sell online, we use search engines, we store digital photos; so we voluntarily leave a comet trail wherever we go. The internet and IT empower us hugely but also put us at huge risk. We are now digital citizens in the digital century.

The Global Digital Universe

These changes are happening everywhere and, as information has gone global, privacy has gone global.

One of the more exciting things about my 10 years as Privacy Commissioner has been to see the dawning of international efforts to bring some order to the wilder frontiers of IT. APEC, OECD, the EU, GPEN, APPA, the International Privacy Commissioners Conference - all are working to provide some rules and standards to protect us in this new world of data. In a very interesting development the United States, via its Federal Trade Commission and Department of Commerce, are stepping up the action. They are recognising that because they regulate the US based global internet companies, they the US regulators, need to take a responsible global view of how they handle these monsters. Both Google and Facebook have recently been fined heavily for breaches, by the FTC. Both are subject to orders imposed on them by the FTC to report annually for the next 20 years against certain standards of behaviour, or risk penalties.

The recent 35th International Privacy Commissioner's conference in Warsaw in late 2013 decided to get in behind the Global Privacy Enforcement Network through which we will help each other to identify misbehaviour and harm to consumers; and then provide redress and impose penalties. We also took some real steps towards a more active coalition of Privacy Commissioners to act globally across a range of privacy issues.

What happened at home?

Back to NZ: What has changed during those years of the new century, up to now?

The digital citizen is nearly a reality; public use of the internet has reached 86% (up from 37% in 2001); IT power and the internet have permeated every corner of our lives. Not surprisingly our polling shows that public concern about privacy issues has grown strongly, from 49% in 2001 to 67% in 2012. 88% of those polled want businesses punished if they misuse people's personal information; 97% want the OPC to have the power to stop a company breaching the Privacy Act; 84% are worried about their children on the internet; and 82% are worried about how business uses their information.

The media have woken up to the fact that they were missing the story of the century and have focused increasingly on privacy and technology stories. Our own media enquiries are up from about 150 in 2003 to over 300 ten years later; and are less trivial and increasingly complex. The likes of the Andrea Vance issue has the media focussing on privacy as a complex, live issue and an essential part of freedom of speech, rather than its enemy. Privacy has been recast as a pressing political issue, rather than a slightly boring compliance issue. Ten years ago, who could have imagined this recent *Dominion Post* headline 'Privacy a Fundamental Human Value' (remember we started the decade as the 'Gestapo').[9]

[9] Editorial in The DomPost, 28 December 2013

Both the public and the media have realised that the changes I have described above in technology, government and business have huge power to help them; but also to intrude on their everyday lives, limit their freedoms and deprive them of choices and control over their own lives. Increasingly OPC has gained profile as a watchdog and a regulator, as of course we always were – but were undervalued for that role.

What else happened? Well, ACC, MSD, and EQC happened. 2012 was a watershed year for data breaches for the public sector.

There were failures on a number of fronts:

1. ACC – email breach in August 2012 – details of 6700 clients leaked.
2. MSD – unsecured WINZ information booths.
3. EQC – email breach

It's also happening in the private sector – think of Telecom/Yahoo/Xtra breach in February 2013 when the email accounts of 60,000 New Zealanders were compromised. This saga is continuing, with phishing, spamming and misuse of the data of hundreds of thousands of New Zealanders which was gathered in the first incident.

What is the cumulative effect? The public woke up to the fact that their information is no longer completely safe with business, on the internet and with government departments - if it ever was.

Along the way from 2003-2013 I should note that we at OPC have been busy; the credit reporting code, data breach guidelines, CCTV guidelines, cloud computing guidelines, material for youth and seniors, for schools, business, the health sector and government; surveys of data transfers and personal storage devices. Early on we set up a small technology team in the office; developed a privacy officers network; Privacy Awareness Week started in 2007. We achieved EU acceptance of our privacy law – an important achievement to open business opportunities for NZ firms. Also along the way our incoming enquiries have risen by 36% and media enquiries have risen 100%; demand for our advice has also risen sharply.
One of the most significant elements has been that in 2011, after 5 years of study, the Law Commission recommended giving the Privacy Commissioner more powers to promote good stewardship of personal information and stronger enforcement powers. These recommendations have taken on new urgency in the light of all of the developments, but especially the data breaches by government departments.

What does it all mean for OPC? Remember the struggling and embattled organisation I came into in 2003? Well, in 2013 we are still small and under pressure, but the climate has changed; our public mandate is much strengthened through public concern and national and international demand for good information stewardship by government and business. We are still under-resourced – in fact our resources are little changed from 2005, but we have rigorously rejigged our priorities to help us to cope. We hope that in the near future the Government will move favourably on both law reform and increased resourcing; we are also empowered by our international colleagues' support; and by the growing willingness of big business and internet corporates to recognise that good privacy is actually good for their business in the longer term.

OPC reviewed against my criteria for ICEs:

- **Independence** - I think we are doing pretty well, perhaps even too well in the eyes of some; it helps that privacy is now a big issue (everything from the Obama/Snowden saga to the fact that dictionary.com declared "privacy" to be its word of the year in 2013); and citizens don't just expect, but demand, independence of us;

- **Effectiveness** - even with limited resources we have innovated and targetted; prioritised and reprioritised; pinched, scraped and borrowed to produce some material for real value - for schools, for cloud computing customers, for employers and local authorities to specify a few;

- **Regulatory and enforcement credibility** - the backlog is gone and we have made some advances in pursuing both mediation and enforcement action more vigorously, for example through special investigations;

- **Service to clients** - the website is miles better, we now answer our freephone line with a human voice rather than an answerphone (reversing the national trend there); I believe our tone and style with clients has moved from legalistic to human;

- **Advocacy** - without a PR person in sight, we have responded to and leveraged off the 100% increase in media interest and calls, to good effect. Privacy Awareness week has been a major public and corporate education process which has now borne good fruit in the responsive reaction from the likes of Telecom and ACC to major disclosures of people's private information; advocacy for the role of the office has moved from an uphill battle to relatively smooth going.

I believe we have evolved in response to huge forces; while still staying true to the principles of the Privacy Act and the fundamentals of being an independent Crown Entity.

The Future

The New Zealand Privacy Act could be said to have started with a round of raspberries from the media; privacy law is now turning into a big bang – even, I suggest, the 21st century human right. All over the world as well as in NZ, privacy regulators are moving up several gears, acquiring new powers, the ability to enforce the law and curb bad behaviour and a new mandate from a worried public to be a watchdog with both bark and bite.

My prediction, and that of many others, is that we are only a small way up the curve of technology and information century changes; the power of digital media just keeps growing.

But generally as a small country, and as users, we are going to be “takers” or receivers of internationally developed products and technologies; all the more important, then, to be active participants in international initiatives to regulate this blooming, buzzing confusion of the digital age; and to have an active domestic regulator and watchdog.

The changes to the Privacy Act will, we hope, soon mean some sharp edges being introduced into the law; e.g. compulsory privacy breach notification, the power for OPC to audit and to require compliance (for example strengthening security safeguards, issuing take-down notices or ordering an agency to give access to information). I hope OPC will continue to encourage the growing majority of willing compliers in the regulatory pyramid; but with increased power to use enforcement against the unwilling, or the genuine rogues.

It is tempting to talk about finding a balance between privacy and security. I strongly believe this is a dangerous path to tread; what we need is a twin pillars approach. We need both security and privacy in our structures and systems; without either one of the twin pillars we will get a distorted and weakened building which will collapse at the first shake.

The long game is about trust. Privacy is as important to people as it has ever been and perhaps more so because they are refusing to have their right to privacy taken for granted. People need to trust the digital environment and they won’t do that unless they are sure that their personal information is being properly safeguarded. In New Zealand the high profile breaches, GCSB Bill, and the Vance/Dunne issue have raised the stakes still further in many people’s minds. The role of an ICE is to underpin that trust and sustain it by

effective regulation. A public belief that wrongs will be righted or perpetrators bought to account is well known to be essential to the credibility and democratic mandate of governments. In the case of OPC, in the transformative digital environment, social and economic growth will be at risk without a public belief that it is a safe zone.

If we don't recalibrate our approach, civil disobedience along the lines of Anonymous, Snowden and Assange will become increasingly common with no real establishment response to allay citizen fears that the rebels have a real point. Ned Kelly was not very smart because he forgot to protect his legs with his armour, and he was a thief and murderer to boot; but in spite of that he became a folk hero because he personified a spirit of freedom, and there were injustices and provocations that people identified with.

I believe the new ethics for business and government, and even social life will be the ethics of good information control.

Individuals must be aware, make choices and retain control wherever they can. Where they cannot, privacy commissioners and governments have to watch, monitor and control (2007 AR).

The challenge is to various players:

- **Crown Entities** – to question and establish the value they aim to provide, and then measure themselves effectively and publicly;

- **Government, Parliament and the media** – to value and respect the status and independence of ICEs by good appointments, balanced resource provision, and intelligent monitoring and scrutiny.

ICEs as independent, effective, answerable entities is the desired outcome. I hope the suggestions I have made will help us to move towards that goal. For the Privacy Commission, we need to be a watchdog with a good set of teeth, able to use them when needed, but generally using bark rather than bite.

What's the answer to the question I posed in the title of this talk - "Constitutional Monitoring or Constant Nuisance"? It's a trick question of course; the answer is both.

Many thanks to my innovative, loyal and industrious crew, without who we could not have guided our little boat through the turbulent decade.

I've enjoyed munching on the fish which various events have caught in our net. But I am happy to hand the net over to my successor, John Edwards.