Roscoe Lecture

12 January 2015

Thank you for those kind words of introduction.

It is a great pleasure and a privilege to address you this afternoon.

I have been asked to reflect on the role of the Information Commissioner.

The Information Commissioner upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals. To list the legislation for which I am responsible – there's the Freedom of Information Act (10 years in operation this month) and the associated access to information regulations – the Environmental Information Regulations, and Inspire Regulations. And on the privacy side, the Data Protection Act and the Privacy and Electronic Communications Regulations, known as PECR. (The Inspire regs are about spacial data and PECR are the rules under which we can take action against the nuisance call and spam e-mail operators.)

But simply to list the list doesn't really answer the question the little boy asked his mother on encountering Randolph Churchill – 'Mummy, what's that man for?'

So what is the Information Commissioner for? And what, for that matter, are information rights for?

Over the past six weeks those are the questions that have been asked by the Ministry of Justice - the Whitehall Department responsible for Freedom of Information and Data Protection. The Information Commissioner's Office – the ICO – is undergoing a process called Triennial Review.

Liverpool has its Biennial. Non-Departmental Public Bodies and Arm's Length Bodies – NDPBs and ALBs or Quangos, to you – have Triennial Reviews. In other words, every three years they are made to justify their existence and their approach. As you will hear, the ICO is in fact neither an NDPB nor an ALB, but I wasn't going to resist accounting for what we do and how we do it. So we've engaged with the Triennial Review process.

This Friday is the deadline for responses to the Ministry of Justice's call for evidence from stakeholders and citizens about the work of the ICO. So today I'm going to try to answer the small boy's question 'what's the Information Commissioner for?' And I'm going to try to answer it in terms of the significance of the work we do, as well as the way we do it. In other words, why all this stuff matters.

But first, if you will allow me, I'd like to say what a particular pleasure it is to be giving a Roscoe Lecture and addressing a Liverpool audience. I am sorry it has taken me more than five years since my return to the North-West to undertake an engagement such as this in the city where I spent four happy years getting my degree back in the 1970s.

I undertook my university studies a little further up Mount Pleasant. Pretty early in the first year of my history course I was introduced to the great William Roscoe. In the Harold Cohen Library, I came across a poll book for the 1806 election in which William Roscoe was the Whig candidate. In those pre-Ballot Act days, a poll book published, not just the speeches of the candidates, but also the names, addresses, and occupations of the voters – and, you've guessed it, how they voted too. So not just pre-Ballot Act, but very much pre-data protection as well.

But back to the essay question.

The business of the Information Commissioner is upholding information rights - the right to privacy and the right to know. These rights are fundamental, but not absolute. Privacy and transparency are to some extent in conflict. They are qualified rights. In other words, there's a balance to be struck – as we've learned in the debates over press freedom and press behaviour in recent months. (The report of your distinguished Chancellor Sir Brian Leveson is something to which I shall return later in this talk.) You can see that too in the debate around the so-called Right of individuals to be 'Forgotten', by Google and other search engines – in reality, the right to have incorrect or out of date personal information de-listed from search results.

Similarly, the controversy surrounding the revelations of the NSA whistle-blower Edward Snowden point up the balance that has to be found between individual privacy and national security.

Let's start with the right to know.

The Freedom of Information Act 2000 came into effect on 1st January 2005 – so we have ten years' experience of the law in operation. The Act gave citizens the right to request access to information held by designated 'public authorities' with certain conditions and certain exemptions. These can be either absolute exemptions – one example would be information derived from the security agencies - or exemptions qualified by a 'public interest test' where the arguments in favour of disclosure have to be set against the arguments against. Qualified exemptions include protection of personal information – which is where Freedom of Information and Data Protection can be thought to collide.

The overriding assumption is that information will be published unless there is a good reason for not doing so. Public authorities have to decide promptly and within 20 working days – or longer if they need extra time to assess the public interest.

A requester who has been turned down can ask for an internal review by a more senior official. And if you still don't get what you want, you can appeal to the Information Commissioner for a decision. That's where my office, the ICO, comes in. We investigate and order publication – or not. And then either party, the requester or the public authority, can proceed to a tribunal and have a further go. And beyond that there can be interventions by Ministers who, in the case of material that falls within their areas of responsibility, can impose an outright veto on publication in 'exceptional cases'. And then the Courts might get involved; that's what has happened in the matter of the Prince of Wales's letters to Ministers. Here the *Guardian* newspaper has challenged the Attorney-General's veto before the Supreme Court. Judgment is awaited.

That's a whistle-stop description of the legislation - but really to understand the ins and outs of FOI you need to consult the Information Commissioner's very informative website at www.ico.org.uk.

Also on that site you'll find some examples of game-changing decisions by the Information Commissioner that forced the publication of information that the authorities initially wanted to stay private - the salaries of senior public servants earning more than the Prime Minister; food hygiene inspection results for pubs and restaurants; MOT failure rates for different models and makes of car. And only last month, the names of private landlords convicted of breaches of health and safety regulations.

What the Information Commissioner can't claim all the credit for is the publication of MPs' expenses claims for duck houses, moat cleaning, or wisteria pruning. In the end, those revelations were the result of a good old-fashioned leak to the *Daily Telegraph* during the protracted toing and froing between the ICO and the Parliamentary authorities over how Freedom of Information should be applied in the case of Members of Parliament. In that sense, publication was a consequence of the Act if not finally the result of a decision of the Commissioner.

What ten years of FOI in operation has taught us is that even where publication is at first fiercely resisted, a Decision of the Information Commissioner can lead to perfectly routine proactive publication of the same data series subsequently. And that's what's happened in all those cases I've just cited – restaurant hygiene, MOT failures, and so on. Even MPs expenses.

It's true that responding effectively to FOI obligations can be burdensome, but, like any other statutory obligation, it has to be done.

Some authorities are better at doing FOI than others. And you can tell a good deal about how an authority is managed by how well they cope with their FOI obligations. Public authorities who make a mess of FOI often won't be much good at meeting their obligations under the Data Protection Act either. Which at least begs the question about what other statutory responsibilities they might be having difficulties with.

Some critics complain that FOI costs too much. That it's a luxury we cannot afford in lean times. I am strongly of the opinion that the net impact of FOI is to reduce costs to the public purse. This is because shining a light into the darker corners of the public service cuts waste and promotes efficiencies that must outweigh the administrative costs involved. But I also believe that the savings to the public purse could be even greater if my office was allowed to spend more on advice and guidance, helping individual public authorities to avoid making the same mistakes over and over again.

The history of freedom of information suggests that the idea is popular with opposition parties, but politicians can go off the idea when in government. I exempt from this observation the present Minister of State, Simon Hughes, who only last week was promoting the idea of extending FOI to cover Water Companies and Housing Associations.

In this connection, I am very pleased with the progress that is being made, under the auspices of the CBI and the Institute for Government, on model contract clauses to cover the transparency obligations that should apply to commercial providers of contracted-out public services paid for by the public pound.

But consider Tony Blair's verdict on FOI. In his memoirs *The Journey*, the former Prime Minister describes the Act as his "biggest mistake" and "utterly undermining of sensible government".

Originally Mr Blair had enthused about "a new relationship between government and people: a relationship which sees the public as legitimate stakeholders in the running of the country". I must say I'm with Tony Blair Mark 1 on this.

The current administration is very keen on transparency and the Cabinet Office Minister Francis Maude is a strong advocate of proactive publication and of the dynamic potential of publishing Open Datasets. But is proactive disclosure on its own enough? I don't think so.

Last month, Mr Maude told the Institute of Government:

> "My aim if I'm honest with you is to make Freedom of Information redundant," he said. "My view is that we should be proactively making public everything that is appropriate."

"Everything that is appropriate": that's the worrying phrase. Who decides? Proactive publication is, of course, desirable – and it also saves money in the long run. After all, why should an individual have to go to the trouble of making a specific request for something that should be freely available to all anyway? But to rely on proactive publication alone leaves the citizen a bit like the supermarket shopper who's told by the high handed store assistant: "if you can't find it on the shelves, we ain't got none". This wouldn't work for a customer focused supermarket and isn't good enough for modern government.

Proactive publication and Open Data must go hand in hand with Freedom of Information access rights. The one doesn't supersede the other. Because not everyone has the same conception of FOI.

Take David Cameron himself in an appearance before the Liaison Committee of select committee chairs back in March 2012:

"It seems to me that real freedom of information is the money that goes in and the results that come out. Making Government transparent is the best thing. We spend, or the system seems to spend, an age dealing with freedom of information requests which are all about processes and actually what the public or the country want to know is how much money are you spending, is that money being spent well and what are the results."

"Publication of information is better than the discovery process which I think does fur up the arteries on occasions," the Prime Minister added.

Now, freedom of information is never going to be comfortable for the powers that be. But does it really fur up the arteries of government?

And what about the charge that FOI means that civil servants aren't keeping proper records? A study by the Constitution Unit at University College London found no conclusive evidence for the oft-claimed 'chilling effect' of FOI on government record keeping. It is much more likely that modern methods of communication are to blame – mobile phones, texts, and so on. And, let us remember, so-called 'sofa government' came in well ahead of FOI.

In fact, the decisions both of the Commissioner and of the Tribunal show that there is indeed respect for the so-called safe space for deliberation and the provision of frank advice to ministers.

History shows that the tide of transparency and accountability is unstoppable, but that it has always been resisted to some extent.

When others of my age were partying or studying, I have to confess that I was sad enough to be collecting signatures on a petition to get the local London borough council where I lived to notify neighbours about planning applications.

What's shocking about that is not so much that that was what I thought a sixteen year old ought to be doing, but that publishing such information was not routine. It is now. But it most certainly wasn't then.

Today, we expect things to be open and transparent – and there's a row when they aren't. Forty years ago the opposite was the case.

I've recently recalled how, as a member of Liverpool City Council in the early 1970s, all council papers were marked 'private and confidential' ahead of any decision - thus making consultation with those affected impossible. I got into a good deal of trouble for making public a report on a plan to relocate the polytechnic, as it then was, to a green field site in my ward - ahead of any decision. I had to write a formal letter of apology in order to avoid formal censure by the council.

We've come a long way since then – and a long way in the last ten years, thanks to the Freedom of Information Act.

Now let's look at the other dimension of my responsibilities – the right to privacy. In the UK, the original Data Protection Act was passed back in 1984. Back in the late seventies there was building concern about the increasing power of computers to compile detailed and very personal information about individuals, to enable large databases to be amassed and to use this information in ways that were unwarranted. Of course, computing looked very different back then in the days of mainframes, glowing valves and whirring magnetic tapes. There was no internet or mobile devices, no server farms or cloud computing.

But even in that distant world of very limited computing, the effect on privacy was an emerging concern. And there was also the fear that, without safeguards, the public would not embrace the benefits that new technology could bring - out of fear and mistrust. Rings a bell? Those fears and the need for safeguards are even more relevant today.

And over these thirty years we've seen the data protection principles, the safeguards contained in those early laws - fair and lawful processing, purpose limitation, security, limited retention of data, right of personal access and correction, safeguarding of international transfers, and so on – being taken forward. The 1995 Data Protection Directive – 95/46/EC, another of this year's anniversaries – led to the 1998 Act and, incidentally, to the transformation of the Registrar into a Data Protection Commissioner and then into the Information Commissioner. And Data Protection's importance was underlined when it was included as a specific fundamental right in the EU's new Charter of Fundamental Rights

Today that 20 year old Directive is scarcely fit for purpose as the technology and the uses of data have raced further ahead of anything the law makers envisaged. The institutions of the European Union are moving, but at a snail's pace, to reform the data protection regime with a new Regulation which would apply uniformly across the single market. And Data Protection Authorities like the ICO have to work beyond Europe's borders to deliver global responses to global threats.

No use sitting around complacently in some kind of Fortress Europe when a Russian website, registered in an Australian territory, with a domain name acquired in the USA, is streaming around the world live pictures from UK domestic webcams with inadequate password protection – or was until the ICO, and the Canadians, the Australians, the Americans and the authorities in Hong Kong and Macau got together and put a stop to it.

When I started as Information Commissioner in the summer of 2009 I knew I was coming to do an important job. But I'd come from the world of advertising standards regulation where every week some cheeky ad or other was causing a stir. I was expecting life at the ICO to be a bit more sedate. How wrong I was.

The almost universal adoption of online communications, smart phones and other mobile devices, and the development of new applications to service the growing market raises all sorts of questions about the control we have over our own data. It has also encouraged governments to get involved – wanting to deliver services online by default and sometimes wanting access, in the name of security, to what we thought was private.

Whatever we do online, we are leaving a trail of personal data which can be analysed, linked, mashed, and crunched. And our privacy is more and more compromised. Some people say, hey that's the modern world. Get over it. But it doesn't have to be like that. Sensible laws and sensible citizens can protect privacy and still enable good things to happen online. And sensible data controllers too understand that customers will fall out of love with companies and brands that do not respect either their privacy or their intelligence.

You can have the good things of digital services without the bad things, but we have to be realistic about what the law should do and what individuals should do to safeguard their own privacy. The laws have to be practical and realistic – and not tie data protection authorities like mine up in knots attempting to enforce over-spec'd procedural obligations when the emphasis should be on promotion of good practice for data controllers and consumers - with proportionate, risk-based enforcement where things go wrong.

And citizens and consumers need to be much more savvy about what is really going on when they access online services.

There's a major piece of work for the ICO going forward, raising awareness, providing advice, promoting privacy by design and privacy by default. Why do so few consumers take the trouble to set strong passwords matters when they wouldn't dream of leaving the front door unlocked or their keys in the ignition? Why were those webcams being sold without a privacy setting that made the customer change the default password to get started?

And then we're back to the old question of finding the balance. The right to privacy or the right to know? This or similar policy dilemmas arise with all sorts of government initiatives designed to drive efficiency in the public service. Promoting more extensive data sharing between public authorities. Sounds like a good idea, but only if the privacy risks have been assessed.

The care.data plan for uploading patient information from GP surgeries to the Health and Social Care Information Centre depends crucially on citizen confidence – which, following last year's botched communications exercise, is in short supply. And yet knowing which treatments work and perhaps which GP surgeries are prescribing efficiently and effectively – and which aren't - seems to make eminent sense, particularly with a health service which is facing ever increasing demands, and levels of resourcing which aren't keeping up.

And then there's the continued uncertainty around the proper supervision of the surveillance activities of the security services following the Snowden revelations of 2013. Because the Data Protection Act specifically exempts anything that would affect the safeguarding of national security, this responsibility has never fallen to the Information Commissioner. The Regulation of Investigatory Powers Act (RIPA) has its own inspection regime.

I do not underestimate the real challenges posed by international terrorism – particularly after last week's shootings in Paris. Truly, nous sommes tous Charlie. But, thinking about Paris, and the Woolwich murder too, we need cool heads to analyse carefully what information the security services had access to and how they used it before necessarily concluding that we must give them access to more and more of our private information.

We must avoid knee jerk reactions In particular, I am concerned about any compromising of effective encryption for consumers of online services.

Every week, we hear about cybercrime and online services being hacked. And we read about the threat of cyber warfare. Citizens, businesses, and nation states need to protect themselves. Internet companies are understandably offering their customers online services that are better encrypted following recent security incidents.

Last week, the head of MI5 Andrew Parker made a speech in which he said:

"We all value our privacy and none of us want it intruded upon improperly or unnecessarily. But I don't want a situation where that privacy is so absolute and sacrosanct that terrorists and other who mean us harm can confidently operate from behind those walls without fear of detection."

Hear, hear. But neither do I want a situation where the security imperative closes down every debate about rights and obligations. The dictum 'Salus Populi Suprema Lex' can be translated two ways. Either 'the common good is supreme' or 'state security calls the shots'. Either way, it's about determining where the public interest lies.

In November, following the report of the Intelligence and Security Committee of Parliament, Facebook were as good as accused of sharing responsibility for the murder of Fusilier Lee Rigby and the boss of GCHQ spoke of some of the internet giants being 'in denial' about being 'the command and control networks of choice' for international terrorism. Robert Hannigan said that privacy isn't an absolute right. Nobody said it was. But, in matters of security, we surely need an effective American-style Privacy and Civil Liberties Oversight Board or the equivalent to find the right balance.

A year after I made a submission to the Intelligence and Security Committee on the subject of consumer encryption and oversight arrangements we are still waiting for the Committee to report.

It is, however, encouraging to see the oversight issue at least being addressed in the Counter Terrorism and Security Bill. It is also encouraging that the Government is currently consulting on setting up a Privacy and Civil Liberties Board. We will though need to be sure that what is proposed really would provide effective and balanced oversight.

So in answer to the question 'what are information rights for?' I'd say the debates around the right to privacy and the right to know are of central importance to the way we live in the 21st century in a modern liberal democracy.

And finding the balance when those rights are in conflict provides part of the answer to my other question, what is the Information Commissioner for?

Now, I've used the terms Information Commissioner and Information Commissioner's Office or ICO pretty much interchangeably in the course of this lecture. In fact, they are not quite the same thing.

The Information Commissioner is the legal entity empowered by information rights legislation. I carry the responsibility for upholding the legislation. The ICO are the almost 400 staff who assist the Commissioner in carrying out his duties. In other words, they do the work and I carry the can.

I am a 'corporation sole', appointed by Her Majesty the Queen, but I have a £20 million operation behind me to do the work. Sir Brian Leveson suggested that consideration should be given to reconstituting the ICO as a commission with several commissioners. In the context of the Leveson Inquiry into Press Standards I think the point was that, back in 2003 or whenever, the ICO had perhaps not displayed enough rigour – or vigour, even - when considering how best to apply the Data Protection Act to the newspapers. It's not at all straightforward, by the way, because of the specific exemptions for journalism, but we've recently published clearer guidance on the subject – in response to another Leveson recommendation.

A commission with commissioners is one of the ideas being examined in the current Triennial Review. Any re-constituting of the ICO would follow the completion of my term as Commissioner in June next year so I can be thoroughly dispassionate about it. I think it's a rotten idea. The suggestion that decision making within the ICO is not already collective is mistaken and our management board, including non-executive members, oversees corporate governance issues. But appointing, on top of the expert and experienced staff, more commissioners to argue things out would only lead to delays and increase costs without any benefits that I can see. We have many, many stakeholders. We listen to them. We will continue to work hard to understand and respond to their concerns. But this does not mean that their specific interests should be directly represented within a board of commissioners.

Whether or not the 'corporation sole' model is to continue, I believe three other factors will be vital if the ICO is to be able to continue its work effectively:

- Independence
- A robust funding model
- The regulation of both privacy and access to information within one agency.

First, independence. The Information Commissioner must be independent of all interests in order to do the job Parliament has given him to do. Sometimes, it's about telling inconvenient truths to powerful people. Of course I am independent. The Directive says data protection authorities must operate with complete independence. I'm appointed by Her Majesty the Queen. I can only be dismissed by the Queen on joint resolution of both Houses of Parliament. I make an annual report to Parliament. Sounds pretty independent.

But although the Commissioner is not one of those Ministry of Justice Non-Departmental Public Bodies or Arm's Length Bodies I was telling you about, I might as well be so far as our relationship with our sponsoring department is concerned for all the returns I have to make and the departmental policies with which I am expected to comply.

A much better arrangement than sponsorship by the Ministry of Justice would be reporting direct to Parliament. The recent report of the Public Administration Committee made the case for all 'constitutional watchdogs', including the Information Commissioner, becoming Officers of Parliament. If that works for the Parliamentary and Health Service Ombudsman or the Electoral Commission, why not the Information Commissioner?

This line of reporting has long been championed by the Commons Justice Select Committee. I wasn't convinced when I was interviewed by the Committee at my appointment hearing in 2009. But experience has taught me that independence, like justice, has to be seen to be done.

Next, a robust funding model. And this isn't me rattling the tin. I know all public bodies are under pressure. I know the job of balancing the books will continue after the general election, whoever wins. I am talking about something else – and it follows from the independence point.

The case for a different funding model for the ICO arises from the need to resource the regulator in a way that encourages good practice and penalises bad practice. The problem for the ICO is that the proposed Regulation would remove the obligation on those processing personal information to Notify with the ICO. All those thirty five pounds notification fees – and a few five hundred pounds from the biggest players – bring in the almost seventeen million I need to run the data protection side of the operation. I'll still need a register of processors if I'm to enforce the new rules. Anyway, I think the polluter pays principle is a good one. But Parliament is going to have to move fast to make sure the regulator is equipped to implement the new rules effectively – as soon as the folk in Brussels have reached agreement.

Another problem for me is the funding of our FOI work which cannot draw on the income from data protection notification fees. FOI is funded by a grant-in-aid from the Ministry of Justice – and the grant has been cut every year since I've been Commissioner. One of the attractions of reporting directly to Parliament is that the ICO could break free from the purse strings of the Ministry of Justice – and its apron strings too. I don't kid myself that direct funding from the Treasury would be a bed of roses, but, combined with Officer of Parliament status, we might be able to secure the level of funding that would make a real difference to the way in which the FOI system operates.

The experience of the ICO over the past five years is that if public authorities know you are on their case the whole system speeds up dramatically. And with more money for FOI, we could start delivering on the FOI side of the business the same levels of advice and guidance which are now absolutely standard for data protection.

And that gets me to the third point on my list: the reasons for the continued regulation of both privacy and access to information within a single agency.

Information rights are more and more a seamless garment. As we've heard, there are data protection considerations to be taken into account in many FOI cases. Similarly, there are access to information considerations that impact on data protection cases. The ICO is able to address both aspects of a case within the one organisation. That is a good model, and one that is being adopted elsewhere as other countries introduce information rights legislation, adding an access to information law to an existing data protection regime or legislating for the right to privacy where the right to know is already established. It must be more efficient to have these issues resolved within a single body than to establish separate regulators for rights that are so interdependent. Where privacy and access to information are handled by different regulators the result is mounting cost, and issues that could have been resolved by a single regulator being handed to the courts to decide, reconciling the often conflicting views of two rival authorities.

It remains to be seen what the Triennial Review process will produce. Certainly, we are always open to new ideas for doing things better. And the next 18 months are going to be exciting.

I sometimes wonder how things would have turned out if, back in 1973, I'd taken up the suggestion of the great Arthur Dooley to go into partnership with him marketing Mersey Mud. You know, to homesick exiled Scousers. It'd be dead easy, he said. All you need is a bucket and a piece of string. Sometimes the job of Information Commissioner can feel a bit like wading through mud – and I could do with more buckets and more string. Sometimes too, it can feel like finding one's way through a Dickensian London Fog. And then I remember that people made money selling tinned London Smog to tourists. But that was before the Clean Air Act - and the Data Protection Act, and the Freedom of Information Act.

Thank you.