4th International Conference of Information Commissioners
MANCHESTER 2006

Tuesday 23 May

Except where indicated, all text has been transcribed from recordings

Page

Tuesday 23 May

Opening remarks
Richard Thomas, UK Information Commissioner

Thank you very much indeed Graham. Could I add my very warm welcome to the so-called wider FOI community of International Information Commissioners – it is a real pleasure to have you here this morning. I wanted to start with a very public thank you to the international FOI Community.

As I am sure you will all know, FOI went live in a real sense in January 2005 in this country. It's been a challenging first year for everybody involved in Freedom of information, but certainly in the run up to January 2005 and subsequently, we have learnt a huge amount from Commissioners and their counterparts around the world, and from commentators, writers on the subject of FOI – a very public thank you to all of you!

I'm going to set the scene for today's part of this event by just focusing on the UK experience. Those of you familiar with the UK situation, please forgive me. You won't hear a huge amount new from me this morning, but maybe others from the international community would like a little more detail about how things are going in this country.

We had yesterday the Lord Chancellor, Lord Falconer, at our conference and he announced the publication of the annual report that Parliament publishes, giving a great deal of detail, statistical and other information about the first year of operation. I believe that's now on the website of the Department for Constitutional Affairs and we undertook yesterday to circulate details of that to all delegates.

I am going to say a bit more about my own office and just a reminder that we have a double role. We have been first the Data Protection Registrar's Office, then the Data Protection Commissioner's Office and now the Information Commissioner's Office, so we have been doing Data Protection for some 21 years in this country and doing Freedom of Information in parallel for a much shorter period.

This next slide is trying to summarise the UK Act in one slide and these are just the headlines of what the British Act is all about. But since 1st January 2005, any person, natural or legal, anywhere in the world can make a request (normally free) for any information held by any of 115,000 public bodies. I know that figure sometimes surprises people but it includes every central government department, every local authority, every part of the public education system, the public health system, police and so on. When you add it all up, some 115,000 public bodies right down to the local national health service doctor's practice. And note the key word there, "held". Any information held by any public authority, which of course means that in effect this law is retrospective, it's information held at the time that the request is

made, even if the information, the documentation, was generated well before 2005.

There is a duty to respond within 20 working days and there is a presumption of disclosure. Yes, there are 23 exemptions, but most of these are qualified, and that means that in those cases if there is a greater interest in disclosing the information then normally that has to be disclosed.

The Information Commissioner, myself and my office, we have the primary role of adjudicating on complaints. Where a requester is not satisfied with the response of the public authority, they normally have to go back to the authority asking for an internal review, the public authority has to reconsider the request, normally at a higher level. If they remain dissatisfied, then they may make a complaint to my office, and we will investigate and we will try to resolve the case either informally or by way of a formal Decision Notice. And if we make a Decision Notice, either upholding the complaint and requiring disclosure or rejecting the complaint, either side can appeal to the Information Tribunal: a special quasi judicial institution which has the jurisdiction to review our decisions on fact, on law, or the exercise of our discretion. Once it has been to the Tribunal or indeed if it does not go to the Tribunal, then any Decision Notice ordering disclosure is binding on the public authority and if it is not followed then it is a matter of contempt of court. So there is really quite a serious sanction at the end of the line and so far we have not had any difficulties with public authorities ignoring Decision Notices.

We have been going now for some 16 months and the report published yesterday reveals that to central government alone there were over 36,000 requests made in that period. We also extrapolate from our own figures across the rest of the public sector - no one is counting in detail how many requests are made across the whole of the public sector to all the public institutions, to all the public authorities, but we estimate well over 100,000 requests were made in that first year alone. The statistics reveal that members of the public are by far the largest single category of requester. There were predictions that it would only be of interest to the media, to interest groups, to companies, but the facts give a different picture that members of the public are the largest single user.

The statistics published yesterday also reveal that some 66% of all requests were granted in full by the public authority, and a further 16 % were not granted in full but were granted in part. We so far in the first 16 months have received 3,300 complaints. We have closed 2000 cases and we have issued 213 formal Decision Notices. There is a word which I am afraid is familiar to Information Commissioners and perhaps Data Protection Commissioners around the world, and it's the dreaded word "backlogs"! And yes, in the second half of that first year, we did build up backlogs of cases, and it is an extremely uncomfortable and undesirable position for anyone to be in when you have got backlogs. But we have learnt a great deal in the first year, we have made changes, we are making further changes to the way we do things, we have some additional resources from the Government and we are

certainly well on the road to tackling the backlog problem but we know we're not alone in this.

This next slide just gives you a flavour of some of the decisions we have made in the first year or so. The left hand column on the slide are those cases where we upheld the complaint the right hand column are those cases where we sided with the public authority and decided they were right not to disclose the information. So health inspectors going into local restaurants, the results of those inspections now made public.

These next two cases are under appeal. I think they will be quite interesting test cases when they go to the Tribunal. The first required disclosure of a quite high level meeting inside the Department for Education in London about the issue of school budgets. We decided there was nothing which fell within the exemptions which required the public interest to justify non-disclosure so we have ordered disclosure of those minutes subject to one very minor redaction in the minutes themselves.

The next case in the Department of Trade and Industry carrying out the investigation into the activities of a company was not willing to tell the company the headline ground on which they were appealing, we thought that the information should be shared with the company, the DTI though is challenging that decision and those both cases will go into the Tribunal later this year.

Another one which is also under appeal (and these are controversial cases), details of the contract between the low cost airline Ryanair and the public airport in Northern Ireland, Derry Airport. The terms of that contract were, in effect, the airline was being paid to fly into the airport rather than the more customary situation of paying landing fees in other parts of the world.

A highly controversial area, the expenses of members of parliament. We have made some progress in this area, now the categories under which payments are paid to members of parliament are being disclosed but there is still further progress to be made in that particular area.

Interesting case which was not appealed, a university in this country in Leicester was accused of allowing students to pass a Pharmacy course with very low pass rates, 21% in some cases, and they were being allowed to pass, there was an internal investigation, there was a request for details of that to be made public. The University claimed a number of exemptions including the commercial interest of the University and perhaps the privacy of the lecturers. When we looked into this we thought the information should be disclosed and the university did not oppose our decision in the end. They have now disclosed the full information.

This involving the interface with Data Protection, with privacy law: the details of the money paid to an interim manager by a local authority. We said that was public money, details of that had to be disclosed by the local authority.

In the other column, a case involving Birmingham City Council where over 100 requests were made by one individual. Birmingham City Council was correct in treating those as vexatious requests and therefore do not have to be taken further.

A very controversial set of minutes involving the departure of the Chairman and the Director General of the BBC a couple of years ago after the so-called Hutton Enquiry following the Iraq war, I won't go into details now but we decided that given the amount of information already in the public domain and given the nature of those minutes, they did not have to be disclosed.

Cases involving the acquisition of Art at the National Maritime Museum a case which has gone to the Tribunal. The Tribunal broadly agreed with our approach in law and in principle, it disagreed with us as a matter of fact. The Tribunal said that when a competition for the acquisition of art was live, there was not an obligation to disclose the details, but once the competition had been finished, once the artwork had been purchased then the information should go into the public domain.

Offences committed by embassies in this country, not just parking offences but much more serious matters, given the nature of the relationship between the Foreign Office and the embassies, given the issues about damage to international relations, we said in that case they did not have to disclose details of the offences, with a very clear message sent to the Foreign Office

that we would probably expect disclosure in the future, once they had established new ground rules with the embassies.

A very large number of requests coming from members of the public to many authorities about details of speed cameras, an ongoing saga. As a very broad proposition, we have said that the locations of speed cameras should be made available but not whether the speed camera is live at any particular point. That, we agreed with the police, would not be in the interests of law enforcement.

Moving on to wider matters of disclosures, not directly involving my office. A headline you see almost daily now is "*…disclosed under the Freedom of Information Act*" and the slide here is one I put together some time towards the end of last year, just a single weekend, all these stories carried in the weekend newspapers, details disclosed under the Freedom of Information Act: Government thinking on a possible freight railway between Liverpool and the Channel Tunnel, disclosure of emails within the Tate gallery in London after its decision to buy a work of art from one of its own trustees for £700,000, details of vaccinations given to the troops during the first Gulf War, details of increases in knife crime, declining school standards, £800,000 spent on investigating the death of Princess Diana in the first year of that investigation, £50,000 a year paid to the wife of the Prime Minister for an armoured car and a driver. Just this morning's Times newspaper, "City of Outlaws leads Crime League" details of which city and which crimes and there

in the middle of the article ‘data obtained under Freedom of Information laws’. Every day we are seeing these disclosures coming forward.

We are very keen always to emphasise the impact not just nationally but locally. There are many, many disclosures being made locally up and down the country. Jjust a few examples: the rating by patients of the services provided by individual doctor’s surgeries, drivering tests (the revelation that it appears to be easier to pass your driving test in one London borough rather than another London borough), health and safety at local swimming pools, details of how some schools in one part of the country are very heavily oversubscribed, and just a couple of weeks ago, the Minister of Defence published a very comprehensive report of interest to every locality, a catalogue of incidents involving unidentified flying objects, a very serious report I hasten to add, published by the Ministry of Defence, which was obtained. It was produced about three or four years ago and was made public under the Act just a couple of weeks ago.

The media are watching and using FOI very closely, here are some examples of the verdicts reached by members of the media:

- the BBC’s verdict on the first year was that in many ways positive - new information of real value is reaching the public for the first time. FOIA has become an important tool.
- The Times newspaper – FOIA is beginning to shine light on areas of public life which some would prefer to keep in darkness.

- The UK Press Gazette which is the newspaper for journalists themselves - FOIA is proving to be a useful tool for newspapers seeking to hold their democratic representatives to account.

(Just to digress, I'm not quite sure why newspapers have democratic representatives but we'll let that one pass!)

- The Independent Newspaper – "FOIA has begun to open doors – but is yet to be fully tested against those in government determined to keep those doors locked".

Moving on, perhaps to set some of the themes for today's Conference, areas which I see of being of particular challenge. Third parties – I think you are all aware of challenges faced where third parties are involved. There is a code of practice under this act, the so-called Section 45 Code of Practice which encourages public authorities to consult with third parties when they are affected by a request. But "third parties" covers both individuals where personal privacy may be involved and businesses where their commercial interests may be involved.

Intellectually, there's quite a neat dovetail with the Data Protection Act in this country. Section 40 of FOIA says in effect that there is an exemption where disclosure of information would involve breach of the Data Protection Principles. Now that sounds fine in theory if the neat dovetailing is intellectually perfect, in practice not at all easy. I've welcomed the fact that I

am the Commissioner for both Data Protection and for FOIA. It means that we have to resolve these issues inside our office. In other jurisdictions I know there could be two Commissioners. There are tensions there – we simply have to work our way through them and make the right decision in each case.

Where the commercial interests of businesses are concerned, one of the exemptions would normally cut in. It says that one of the exemptions reads that "Where there will be prejudice to the commercial interests of another organisation or indeed even the public authority itself, then there would not normally be disclosure". But again this is one of the majority of qualified exemptions and therefore one has to look at the public interest test and apply that in each and every case, an area of very considerable challenge.

There is also an exemption for the formulation and development of government policy, and it's not surprising that exemption exists but it is a difficult one. Frankly, it's not very difficult for most government departments to show that their information - their documentation, will fall inside Section 35. Not all their materials, but a great deal of their material will fall within that exemption. But again we are straight to public interest considerations, and balancing the competing public interests in these cases is never going to be straightforward. Government departments, not surprisingly, are keen to push forward the public interest arguments in favour of maintaining the exemption, in other words in favour of non-disclosure. But we have to examine those, we have to articulate the competing public interest in disclosure, we have to unpack that and then make the balancing test.

And this last bullet point that I have put up here just refers to one of the issues which we are encountering time and time again and it's going to be an issue in some of the appeals I mentioned earlier going to the Tribunal later this year, the so-called "chilling effect" on public administration. If I may summarise, the public authority, the government department will say, well perhaps the information here is somewhat innocuous, maybe there's nothing there which in itself will cause any great damage, but if this were to be disclosed it would have a "chilling effect" on public administration. It will inhibit the free and frank exchange of views between officials and politicians, it will deter people from writing minutes and internal memoranda and so on. Now those of you who have been doing FOI for many, many years will smile and say you've seen this before, it's a familiar set of arguments. I know it's nothing particularly new for us, we're still feeling our way however, and we have to get through these first two or three years with this particular set of issues that arise time and time again and we have to lay down the approach for this country. But we are looking very closely at how the same sort of issues have been tackled and resolved in other countries around the world.

I think my time is up now, I was asked just to give a very short presentation to set the scene. The final slide sets out our emerging impressions as to how we are doing in this country. The law has had a high media profile since it went live. It *is* making an impact right across the public sector, right across from the senior levels to the more junior levels it *is* making an impact. I believe in the vast majority of public authorities it *is* being taken seriously. As

a broad proposition the larger public bodies, particularly when there has been strong leadership at the top have been the best prepared. But sometimes being well prepared means well prepared to disclose information when it's required, but it also means well prepared to withhold information when you don't particularly want to disclose the information. But having said that, we have achieved in this country some very significant and perhaps some very surprising disclosures. It has been resource-intensive. There's no doubt that when the Treasury said a few years ago that this was intended to be resource-neutral, the smiles again appeared on many faces. It cannot be described as resource-neutral – it has taken up a lot of time, effort and energy right across the public sector and we must not blind ourselves to that. The boundaries are being tested all the time – again no surprise. One would like to pick and choose the cases to come in a more orderly fashion – we don't have that particular luxury, we deal with the cases as they come in.

So culture is changing in my verdict, but I would not say the culture has yet changed. Yesterday the Lord Chancellor was asked at this conference to mark this country on a scale from zero to 100 as to where culture change had so far gone. It wasn't altogether clear what the starting point was but he said around about 50%. I think that's a slightly optimistic figure, 50% if you start 10 or15 years ago but starting 3 or 4 years ago, my verdict is more like about 30% but moving in the right direction. Thank you very much.

FOI – A European Perspective
Nikiforos Diamandouros – European Ombudsman

I am very happy to be able to address this conference and very honoured to have been asked to be part of the Fourth International Conference of Information Commissioners. Let me begin with some preliminary remarks about the title that I was given for my presentation, which is FOI – A European Perspective.

The term Freedom of Information, FOI for short, is not much use to the European Union institutions. Instead we speak of transparency or openness. Earlier this month for example I welcomed the Commission's European Transparency Initiative. Although there have been attempts to distinguish between them, transparency and openness tend to be used interchangeably. The best explanation I have heard so far as to why there are two terms instead of one at the European Union level is that transparency was used to translate the French '*transparence',* because the translators were unfamiliar with the English word openness in this context. Another phrase which is widely used in public acts is "public access", especially for governments. This

reflects the strong Nordic influence on how the principle of openness has been put into effect at the EU level. So although the title mentions FOI, let us speak about transparency, openness and public access.

I should also give a preliminary warning about the other element of the title – A European Perspective. It is indeed "a" European perspective, not "the" European Perspective for three reasons – first, 46 countries now belong to the Council of Europe, which has produced useful recommendations and public access to official information of governments. However, I shall focus on the European Union which has 25 members, with two more, Bulgaria and Rumania, scheduled to join and the others knocking at the door. Second, I shall be talking, for reasons that I will explain later, about openness and public access at the level of the European Union institutions rather than at the level of the member states. Finally, the European Ombudsman is only one of the European institutions you might get a different perspective from – other institutions as well, such as for example the Council or the Commission.

I plan to speak for no more than 25 minutes or so, so as to leave adequate time for questions and discussion. In the first part of my presentation I shall explain the significance of openness for the European Union and how it has developed in the 12 years or so since the Maastricht Treaty came into force. Then I shall give an overview of the legal framework for public access to documents held by the EU institutions. This will not be comprehensive since I shall focus only on certain key issues. Finally, I shall explain the system of

remedies which offers applicants an explicit choice between judicial review by the court or judicial review by the European Ombudsman.

To explain the significance of openness for the European Union requires a brief explanation of what the Union is or rather what it is not. The European Union is not a state. It is perhaps best described as a multi-level system of governance. Administration in the member states, at the national, regional and local level have the primary role in implementing many aspects of EU law and policy. The Commission is often described as the European Executive but it is not a government. Although the Commission is in many ways a classic of bureaucracy, much of its relationship with the external world is conducted through networks involving a variety of public and private organizations at different levels. For its part, the Council has not just one but two dual identities. First, it is both super-national and inter-governmental, that is to say it is an EU institution but its structure makes it function also as a kind of a standing process of diplomatic negotiation between the member states through a dense structure of committees.

Second, the Council is a legislative body but it also has an executive role especially in relation to police and judicial corporation and the common foreign and security policy. The European Parliament is directly elected but there is widespread agreement that the European Union as a whole suffers from a democratic deficit, being perceived as elitist and unconnected toward their citizens. Whilst the diagnosis of democratic deficit is widely shared, there is less agreement about the remedy. The idea of a Federal Europe still

has its advocates. Critics point out that preconditions for the legitimacy of a federal structure in particular a European public sphere and a widely shared European identity are currently likely. The Constitution for Europe is an attempt to recognize explicitly and to rationalise the multi-level system of governance that has been created in the European Union over the last 50 years. The Constitution represents not more Europe or less Europe, but an acknowledgement of the Europe that we now have. However, to obtain an agreement even on that has not yet proved possible.

The problems that the European Union now faces, summed up in the phrase 'democratic deficit' were already visible when the Treaty of Maastricht was negotiated at the beginning of the 1990s. Part of the response at that time was a commitment to openness , the idea being that the openness of the decision-making process strengthens the democratic nature of the European institutions and that access to information promotes an informed public opinion by enabling citizens to monitor and scrutinize the exercise of the powers vested in the EU institutions. Time does not permit me to engage in a detailed discussion of the concept of democracy. I will say only that openness and public access to information play an essential role in the pluralist version of democracy which is marked by institutional checks and balances that mediate the exercise of public power and promote its accountability to its citizens, not only at periodic elections, but also between them.

The pluralist conception also maintains a balance between egalitarian and libertarian principles, and provides optimum conditions for the observance of

the rule of law and respect for the observance of rights and obligations linked to it. The quality of a pluralist democracy largely depends on its capacity to offer choices, both political and personal. It is or it should be obvious when choice is most meaningful when those who exercise it have access to the information they consider relevant to their choice. Although there is little, if any, overt opposition at EU level to the idea that openness is linked to democracy in the ways that I have described, there is debate as to the precise legal nature of rights of access to documents and information. Some of the arguments put forward in favour of public access are instrumental for example, meaning that it reduces corruption and increases the efficiency and effectiveness of public authorities as the Council of Europe claims in its 2002 recommendation on access to official documents. Furthermore, although the European Court of Human Rights strongly protects the role of the press in imparting information and ideas to the public, it does not recognize a general duty of public authorities to provide access to official information, nor any right to obtain such information. The fact that there are instrumental reasons to favour public access and also the lack of recognition of public assess as a human right within the European Convention of Human Rights have led some people to argue in substance that public access is merely a policy choice of the legislator rather than a fundamental right. On the other hand, some commentators argue that the case law of the Court of Justice logically implies that public access is indeed a fundamental right under EU law. However, the Court has not (or at least not yet), expressly defined it as such. This is more than semantics. If public access were a fundamental right under EU law, that right would be binding not only on the EU institutions but also on the member

states when they are implementing EU law. EU law obligations on member states to provide public access are limited to specific fields. The most important such field is the environment for which the relevant directive was updated in 2003 to take account of the Aarhus Convention. In its transparency initiative the Commission also raises the question of whether member states should be legally obliged to disclose the beneficiaries of certain EU funds. In general however, the EU legal framework for public access does not apply to the member states and there is a great deal of variety in national laws and practices on the matter.

As I mentioned a few minutes ago, the European Union's commitment to openness dates back to the Treaty of Maastricht. The first Danish referendum in rejecting the Treaty gave added impetus and drive for more openness in the way of enhancing the Union's legitimacy. Shortly after the Treaty had finally entered in to force in November 1993 the Council and Commission adopted a joint code of conduct on public access to documents. Although the code was an important step forward, it had three major limitations. First, it applied only to the Council and the Commission, not to the other EU institutions and bodies. Second, it only covered documents of which the Commission or Council was the author. Documents received from outside, from private parties, other institutions, or member states for example, were excluded. Finally, there was not requirement to produce public registers of documents. This severely limited the usefulness of the rules, particularly the system of governance, marked by extensive reliance on networks and committees that are difficult to mark from the outside or even from the inside.

The European Ombudsman had to overcome the first of these limitations through two own initiative inquiries in 1996 and 1999. These resulted in almost all the other EU institutions and bodies adopting rules of public access. The Ombudsman also dealt with complaints against both the Council and Commission regarding lack of registers. The Council was responsible to inform the Ombudsman that it had agreed to set up a register from the beginning of 1999. The Commission reacted to a draft recommendation to establish a register by accepting the principle but asking for more time. In response, the Ombudsman suggested that public registers could form part of the Commissioner's implementation of Article 255 of the EC Treaty which was introduced by the Treaty of Amsterdam. That Article provides for any citizen of the Union and any natural legal person residing or having its registered office in a member state to have a right of access to European Parliament Council and Commission documents subject to general principles to be laid down by secondary legislation.

In due course, the Commission did indeed include a requirement for public access with a proposal for regulation to implement Article 255 and the measure finally adopted, Regulation 1049, in 2001, includes that requirement. Regulation 1049 of 2001 now constitutes the basic legal framework for analysis of the right of public access to documents held by the EU institutions and bodies. The Regulation applies directly to the Council, Commission and European Parliament, it has been extended ad hoc to cover certain EU Agencies. Many of the other institutions and bodies that have adopted rules

of public access following the Ombudsman's own initiative inquiries, subsequently revised them in line with the principles contained in the Regulation. Unlike the earlier Code of Conduct, Regulation 1049 applies to all documents held by the institution or body concerned including those received from the outside. Article 4 of the Regulation provides for the exceptions to the right of access. Most of the exceptions include a harm test that is to say the exception applies if disclosure would undermine the protection of the interest concerned. Some exceptions are in addition subject to the possibility of an overriding public interest in disclosure. This is the case in protection of commercial interests, court proceedings and legal advice, and the purpose of inspections, investigations and audits. If an overriding public interest exists, then there is an exception to the exception and public access must be granted. There is however, no possibility of an overriding public interest in disclosure as regards the exceptions for public security, defence and military matters, international relations, financial monetary or economic policy and the protection of privacy and the integrity of the individual. A stronger version of the harm test applies to the exception which is intended to allow these exclusions a so-called 'space to think'. The exception applies only if disclosure would seriously undermine the institution's decision-making process. There is also the possibility of an overriding public interest in disclosure.

[short pause in recording]

…a distinction between phases where the institution has not yet finished its thinking. That is to say where it has not yet made a decision on the matter to which the document relates and those where the thinking period is over because the decision has already been made. If the decision has not yet been made, the exception applies to documents drawn up by the institution for its own use and to all incoming documents. If the decision *has* been made, the exception applies only to documents containing, and I quote, "opinions for internal use as part of the deliberations and preliminary consultations with the institution". Given the nature of the European Union, it is not surprising that the interface between national laws on access and EU law should have turned out to be one of the points of conflict in relation to Regulation 1049. The Court has resolved the main controversy in favour of giving each member state the right to veto public access to any document of which it is the author, either at the time of sending the document to an EU institution or subsequently without giving a reason. This right applies not only as regards contributions to policy-making but also to documents which the member states submit to the Commission when the Commission is investigating a possible violation of EU law in the so-called Article 226 process.

Another question which proved controversial but which has now received judicial resolution, concerns opinions of the legal services of the institutions. In a special report to the European Parliament the Ombudsman took the view that the exception for court proceedings and legal advice should only apply to the opinions given by the legal service of an institution in that conflicts of possible future court proceedings. In contrast, opinions from a legal service

prepared during the process of drafting legislation should, according to the Ombudsman, be exempt from disclosure only if they fell within the exception protecting the institution's 'space to think'. This would have meant that once the legislation was adopted, public access to legal service opinion would be subject to the seriously strengthened version of the harm test, with a possibility of an overriding public interest in disclosure. The Court however, gave a different interpretation in a government case holding that the court proceedings and legal advice exception applies to *all* legal service opinion. The Ombudsman therefore suggested to the European Parliament that no further action be taken of the special report and in accordance with the Court's interpretation closely could lead into another complaint in which a draft recommendation had been based on the same reasoning as the special report.

As I mentioned earlier, Regulation 1049 contains an obligation on each institution to provide public access to a register of documents. In a case that I decided at the beginning of this year the complainant alleges that the Commission's register of documents is incomplete. In his opinion, the Commission has accepted in effect that it does not yet have a comprehensive register. It said that it had begun by listing documents about its legislative activities, that the coverage of the register would be extended gradually. It added that there could never be an exhaustive Commission Register given that the definition of a document in the legislation is extremely broad. I found that these general remarks did not justify the shortcomings pointed out by the

complainant as regards the documents involved in the complaint and made a critical remark on this point.

Finally, the relationship between public access and data protection was expected to produce controversy. In practice however, few problems have arisen. Last year, the European Data Protection Supervisor Peter Hustinx, who is among us today, produced an excellent paper on the relationship. Since we will have the privilege of listening to him this afternoon I will not develop the subject in my presentation.

As regards procedures for making an application for access and remedies against a refusal, Regulation 1049 retains the system established under the Code of Conduct. There is a two-stage administrative procedure for making application. An initial application, followed by a confirmatory application if access to the documents requested is not provided. The time limit for both initial and confirmatory applications are 15 working days, with a possible extension of a further 15 working days for an application relating to a very long document or to a very large number of documents. If a confirmatory application is refused in whole or in part, the applicant has a choice of remedy. He can either seek judicial review of the decision or complain to the European Ombudsman. In practice, the Ombudsman and the Court receive roughly comparable number of cases. The latest comparable statistics available of 2004 were 9 cases were lodged with the Court, while the Ombudsman made decisions on 11 complaints. Last year, I made 14 decisions under Regulation 1049, of which 11 concerned the Commission, 2

the Council and 1 the European Parliament. Two further cases concerned the application by the European Central Bank and the European Investment Bank of their own rules on access to documents.

As for who chooses to complain to the Ombudsman, putting the figures for 2004 and 2005 together there were 14 complaints from NGOs, 10 from individuals, 1 from an industry association and 2 from companies. The availability of an alternative remedy with different characteristics allows applicants to choose the appropriate remedy for their case. Two obvious advantages of choosing the Ombudsman are that the service is relatively quick and free to the complainant. The most obvious advantage of the judicial review is that the courts decisions are legally binding. They can therefore give authoritative rulings on questions of legal interpretation. Whereas the Ombudsman's interpretation of the law is not binding. Not having the power to make legally binding decisions, the Ombudsman's effectiveness is ultimately based on moral authority and the ability to persuade public opinion. Since the European institutions are sensitive to the need to improve their relations with citizens, I find the prospect of adverse publicity is quite effective at encouraging them to comply with my recommendations.

There are also certain positive advantages for complainants flowing from the fact that my decisions are not legally binding. These advantages concern both the criteria of review and procedure. I shall develop both aspects in more detail, beginning with the criteria. The mandate of the European Ombudsman is to enquire into maladministration. The European institutions

and bodies must respect the rule of law, so if they act unlawfully this is maladministration. However, the converse is not necessarily true because the principles of good administration require more of the institution than merely avoiding unlawful behaviour. As I like to say – There is life beyond legality. Let me give you two examples to illustrate what I mean. The first concerns access to information as opposed to documents. Regulation 1049 is about public access to an existing document, it does not require the institutions to create new documents containing information that someone would like to have. A few years ago however, the Ombudsman drafted a code of good administrative behaviour, which contains among other things an obligation to provide members of the public with information on request. Such an obligation cannot of course be absolute. A principle of good administration amounts essentially to the presumption that information should be provided unless there is a good reason not to do so. Last year, I applied this principle to a case where the complainant had asked the European Central Bank whether it had intervened to soften the fall of the value of the US Dollar and the rise in the value of the Euro. I took the view that if the Bank was not prepared the release this information, it should provide the citizen with sufficient and specific reasons to show clearly and unequivocally its reasons for the refusal. The Bank did indeed provide such reasons and I found no maladministration.

The second example which shows that illegality and maladministration are not necessarily identical, is a complaint made against the Council concerning the fact that it does not always meet in public when legislating. I took the view

that the principle of Article 1 Paragraph 2 of the Treaty of the European Union that decisions should be taken “as openly as possible” applies to the Council. The Council’s own past actions made clear that steps to increase the transparency of its legislative activity had to and could be taken under EU law as it currently stands. Since the Council gave no valid reason why it should not meet in public whenever legislating, I found maladministration and made a special report to the European Parliament which adopted the resolution of proving my recommendation that the Council should review its position.

As regards procedures, I have already mentioned the Ombudsman’s power to conduct own initiative inquiries which led many EU institutions and bodies to adopt rules on access to documents. The considerable flexibility of the Ombudsman can also be valuable to individual complainants. In one case for example, an NGO made a rather generally phrased application to the Commission for access to documents concerning certain negotiations in the World Trade Organization. The outcome of the complaint was a friendly solution in which the Commission supplied the complainant with a full list of the relevant documents so facilitating a more precise application.

Two further examples are provided by cases in which the Commission refused to give the complainant access to a document from a member state. In one of the cases, the document concerned was the response of the United Kingdom authorities to the Commission’s request for information in an Article 226 investigation request, infrequent procedures. The other case concerned a letter sent to the Commission by the Portuguese Minister of Finance in the

framework of the excessive deficit procedure. In dealing with these cases last year, I adopted a new approach. As well as asking the Commission for an opinion, I also asked the authorities of the relevant member states to give me their views. In both cases, the result was that the Commission changed the position, and agreed to provide access to the documents concerned.

In conclusion, I would like to emphasise that although I have focussed on the Ombudsman in discussing remedies the right to a judicial is a fundamental guarantee of the rule of law. The availability of judicial review as a remedy is less essential to establish the publish access as an enforceable legal right at the level of the European Union. The Ombudsman's role is complimentary to the court, providing an alternative remedy that applicants may choose if they consider it appropriate for their case. As I have mentioned, the Ombudsman's effectiveness depends on moral authority, persuading public opinion. This implies that the institution works best in a democratic environment. Furthermore, the Ombudsman not only provides respect for legal rights and hence the rule of law, but also develops and applies principles of good administration. These principles provide, in the shortened phrase that I have already used, a kind of life beyond legality. In my view, they are closely linked, or perhaps even derive from the democratic idea that public institutions exist to serve the citizens and not vice versa. I have no time to develop this argument now, but I would be very glad to develop it in the question and answer period. The Ombudsman thus struggles through the rule of law and democracy in an institutional sense, while the principle of openness links them at their conception. I therefore find it particularly fitting that individuals who

wish to profess a refusal of access to documents or information at the EU level have a choice of remedy. I also believe that as the European Ombudsman, I have a special responsibility to tackle the democratic deficit by encouraging openness whenever possible.

Thank you for your time.

4th
International Conference of
Information Commissioners
MANCHESTER 2006

Secrecy vs Security: the Jigsaw Effect

Air Vice-Marshall Andrew Vallance, Secretary of the (UK) Defence, Press and Broadcasting Advisory Committee

(text of speech supplied)

It's a great pleasure to address this very important conference. I speak to you today as the Secretary of the United Kingdom's Defence Press and Broadcasting Advisory Committee, an independent body which provides guidelines to the UK media on the disclosure of national security information.

I've been asked to speak to you on the subject of 'Secrecy vs Security', an intriguing title. The use of the term 'versus' - suggesting that 'secrecy' and 'security' are somehow inevitably in opposition - reminded me of a famous book called 'Animal Farm'. Written in the mid-1940s by George Orwell, perhaps the greatest British political literary satirist of the 20th Century, 'Animal Farm' is a biting parody of state over-control, using Stalinist Russia as its implicit model. As those of you who have read it will readily recall, the book begins with a rebellion by the animals of Manor Farm who feel they are being

oppressed by the owner – Mr Jones. The rebellion against Jones is led by the pigs, the cleverest of the Farm's animals, who rename their community 'Animal Farm'. They announce that 'all animals are equal' and coin the slogan 'four legs good, two legs bad'. But after its high-minded beginning, Animal Farm follows a seemingly inevitable course towards inversion and reversion, with the pigs progressively controlling the other animals in the same way as Farmer Jones. In the end, the pigs move into Jones' farmhouse, learn to walk on two legs, alter the Animal Farm doctrine to 'All animals are equal, but some are more equal than others' and change the Farm's slogan from 'four legs good, two legs bad' to 'four legs good, two legs better'.

I'm won't test your patience today by trying to argue 'security good, secrecy bad', and certainly not 'security good; secrecy better'. The world is far too complex for such simplistic, good/bad, right/wrong judgements, even if I did believe that security and secrecy were necessarily alternatives: which I do not. But what I would like to offer you today is why I believe that security and secrecy can be both complementary and opposing concepts, depending on how they are implemented. The message I offer is 'security good; secrecy also good' at least at certain very specific times, in certain clearly defined circumstances, and provided that how and when secrecy is imposed, it is done so with common sense and moderation and tempered with proper instruments of oversight and public accountability.

Contemporary British society has a dialectic view of secrecy. The British people see personal secrecy – privacy it is generally called - as an inalienable

right, part of the nation's birthright a fundamental component of their freedom. The introduction of measures seen to erode it are attacked widely and with full force as a matter of the highest principle, with the default setting always protecting personal privacy – except in cases of the most dire and immediate national emergencies. Pressure groups - such as *Liberty* - exist specifically to champion that cause and do so with great energy and determination and much popular support. 'Privacy' is indeed the word in general use here rather than secrecy, but the two in this context mean the same: the right to hold back from the public domain information about an individual that he or she wishes to remain a personal secret. In Britain, the right to personal secrecy is safeguarded in law - *inter alia* - by the Data Protection Act of 1998 and Article 8 of the Human Rights Act also of 1998. Journalistic secrecy is similarly seen as being critical to personal freedom through its role in ensuring that government is accountable. Journalists, and on occasion editors, or even (on at least one famous occasion) a CEO, are willing to risk public censure, even prison, to preserve their secrets, and most notably the identity of their sources.

But in the context of public governance, secrecy has an almost entirely negative popular resonance within Britain. Indeed, it is often presented as posing threats that extend well beyond the obvious areas of personal or collective freedoms, to prosperity, continued employment and individual ways of life. One could sum up the British view of secrecy as 'Private secrecy good, but public secrecy bad'.

Part of this comes from our cultural legacy: the apparently innate British preference for individual freedom and our historic suspicion of centralised government, wherever it might be based. But this preference has been mightily strengthened by the knowledge-centric society in which we now live. Information management techniques play an already dominant and still swiftly growing part in all our lives, and secrecy can often seem incompatible with this. For example, one of the key enabling policies of any system which seeks to impose secrecy – be it personal, commercial, military or governmental - is that of 'need to know': this aims to restrict the type and quantity of information released to individuals to that which they really need. The theory behind 'need to know' is that it reduces the danger of, and limits the damage sustained through, security breaches, compromise or betrayal. But there are growing problems with 'need to know'. Even if one agrees with the principle, which many do not (at least when it is applied at the collective level), 'need to know' involves making highly subjective judgements. No one really knows what they (or anyone else) really need to know, until – that is - they need to know it. Indeed, deciding what people need to know is one of the most fundamental challenges facing knowledge management development. It is also a very convincing reason why people should be at liberty to search the full extent of the knowledge spectrum, as and when the need arises, to find out the particular information they need. And secrecy can only hinder that search.

But of even greater concern to the majority is the potential to exploit secrecy to abuse power. There is no question that a general culture of excessive secrecy holds serious threats to us all. Knowledge is power – today far more

than ever before. And the denial of information, however obscure, is seen by some as reducing their power, while the hording of it by others is seen as increasing theirs. Secrecy in whatever form denies access to information which some believe to be public property by right. Secrecy applied selectively can lead people into making flawed judgements because they do not have all the pertinent facts. Applied in blanket form, it raises concerns that whole areas of government activity are being shielded from proper public scrutiny and accountability. In both forms, secrecy can erode trust in authority, appear to set one group in society above and beyond the others and raise concerns that individuals in Government, or even whole Government departments, may be out of proper control and unaccountable.

Setting aside these objections of principle, there are also some very practical difficulties in keeping secrets secret. Firstly, there is cost. Secrecy is a very expensive business, and the wider the range of secrets that have to be kept, the more difficult they become to manage, administer and police. Secrecy imposes widespread and diverse burdens on the administrative machinery which add time and cost to government processes without adding any apparent value to the products. So much so in fact that whichever preferences a government may have, its ability to impose secrecy will be limited by the capacity of its administrative machine to manage the associated procedures, absorb the constraints and still work at an acceptable level of efficiency.

Allied to that, and of rapidly increasing importance, there is the World Wide Web. The internet has become an information gathering and dissemination

tool of unprecedented capacity and - outside of China at least - available to all in a pretty well unfettered form. The already awesome power of the internet is fed only in part by the already colossal and still rapidly growing capacity and power of the international media, now more closely integrated (at least at the technical level) than ever before. A story reported in an obscure journal in a remote region can be picked up and within hours be repeated all over the World. It then remains on the Google and Yahoo data bases where it can be accessed for evermore. Once there, the use to which it can be put cannot be restricted and can damage both collective and individual security. The terrorists who carried out the London bombings of 7 July last year – for example - appear to have gathered the information they needed to make their bombs from the World Wide Web without external assistance.

The challenges posed by the World Wide Web to those who seek to keep information secret apply not only to individual pieces of information (which can now be posted by anyone for example on web-logs or 'blogs'), but also to what can be learned through aggregation. The traditional modus operandi of intelligence officers - to gather seemingly innocuous information, assemble it into a coherent mosaic and then make sensible judgements from the picture that emerges - can now be performed to a surprisingly high level of competence by anyone with the time, wit and inclination who has access to an internet computer. Sometimes called 'the jigsaw effect', this phenomenon can lead civil or military bureaucrats down the path of even greater and more unproductive secrecy in an attempt to spot information which could form some part of a future sensitive jigsaw.

Of course, like a real jigsaw, one assembled with pieces from the internet does not always produce a true picture. Sometimes, the person assembling the jigsaw forces the individual pieces together to make the picture he believes to be the right one, whether or not it truly matches that on the outside of the box. Sometimes he feels that pieces are missing, when instead they are all there but have been wrongly assembled. Nevertheless, critics of official secrecy do have a point when they argue that the 'Web' now ensures that no secret is inviolable and thus efforts made by Governments to preserve official secrecy are ultimately likely to prove futile. But equally, governments can point out that there is no obligation on them to assemble - or even make a gift of key pieces - of jigsaw puzzles which might then be used to inflict death and injury on the people they are charged to protect. Whatever one's views are on this, I don't think that anyone doubts that the 'jigsaw effect' is a powerful factor; the dispute is centred on whether its effects are more 'good' than 'bad'.

Another practical constraint on secrecy is the public's willingness to accept it. This is not so much 'whether or not?', but 'how much the market will bear?' In Britain, the answer to that question is 'not very much'. Moreover, attempts to extend secrecy tend to strengthen the determination of those claim to champion liberty and who seek to expose 'the truth' as they see it, regardless of the consequences. Little or no general opprobrium now seems to be attached in Britain to the selective leaking of secret government papers; not a Sunday goes by without the publication of extracts from some leaked official document or other. Even when the 'leaker' is found (which is not often, given

the nature of information distribution systems and the ability to take copies even with a mobile phone) he or she is often portrayed as a hero: someone who has taken a stand on principle against those who are seeking to deny to the public information which is rightly theirs. It is somewhat paradoxical that as freedom of information has expanded, conspiracy theorists have become ever more prominent. Perhaps we should not be surprised by this for secrecy arouses people's fascination, and attempts to shape the news – 'spin' – are widely resented. Official denials are now taken almost automatically by those who love 'cloak and dagger' stories as confirmation that what is being denied is in fact true; one often hears the slogan 'never believe anything until it is officially denied!'

The 'whistleblower' mentality holds that it is morally indefensible to keep information from the general public which in any way concerns them. Such a view fails on two counts. Firstly, it ignores the misuse to which certain types of information can be put by individuals or groups willing to use violence to achieve their aims. And secondly, the leaker rarely - if ever - has all the pieces in the jigsaw puzzle and, thus, lacks the 'full picture'; he/she cannot judge the range of the consequences which might flow from the information released. For example, publishing details of the timing, scope and location of imminent military or intelligence operations can warn the enemy, allow them to prepare and lead directly to loss of friendly lives, not only for those actually involved in the operation, but also – as a direct consequence - the lives of those who the operation was designed to protect. Another example is the measures put in place to protect people (both military and civilian) against – say - terrorist

bomb attacks. If the terrorist knows exactly how an installation is protected, he can invariably find a way around the defences.

Perhaps I can best illustrate the need for a measure of secrecy by examining the Secret Services – arguably the most sensitive institutions of any nation. In Britain there are three Secret Services: the Security Service (more often called MI5 - which deals with domestic security), the Secret Intelligence Service or SIS (of James Bond fame and more often called MI6 - which deals with overseas human intelligence gathering) and the Government Communications Headquarters or GCHQ, which intercepts communications. All three of these Services are established by the law of the land, are publicly accountable (if not directly then certainly to the public's representatives) and are subject to careful parliamentary and judicial oversight.

These Services operate in a world of enduring fascination to the public, but they depend on secrecy to do their job of protecting the British people and the people of allied and friendly nations against a wide range of current threats. These threats include – inter alia – terrorism in all its many forms, illegal narcotics, mass people trafficking, organised crime and the proliferation of weapons of mass destruction, in addition to the more traditional counter-espionage role. The details and even the very existence of their operations - future, present and even past - and the identities of those who work for them, have to be protected by very high secrecy levels.

The possible consequences of such secrets being compromised were shown

around the turn of the year when a Greek newspaper published what it claimed to be the name and photograph of the British SIS Head of Station in Athens. This was followed two weeks later by the Russian state broadcasting service showing footage of what it claimed to be four British SIS officers in Moscow accessing supposedly secret information from a transmitter receiver device disguised as a rock. These were not isolated incidents. Indeed, a cottage industry has developed in recent years – no doubt partly at least as a reaction to Secret Service secrecy - to publish the identities of Secret Service agents for the whole world to see. Such ‘secret agent spotting’ is generally looked on as some form of harmless game that embarrasses the bureaucrats and shows how clever the agent spotters are.

But it is not a harmless game. The Secret Services have to maintain a strict ‘neither confirm nor deny’ policy whether or not the person so named is one of their people. Even if that were not so the ‘never believe anything until it’s officially denied’ philosophy means that an official denial would probably be pointless. Persons named as Secret Service officers or agents are often totally separate from the Secret Services, but they and their families suffer just as badly. Whether true or false, public naming damages a Secret Services’ reputation for being able to keep its own secrets; it undermines the Services’ confidence, weakens its morale, and through that erodes personnel retention and recruitment. The collection of secret intelligence from sensitively placed human sources depends crucially on maintaining their confidence. This relationship is always very delicate and can be damaged when identities are disclosed. Naming – whether true or false - deters potential informants from

contact with officers for fear of exposure. Officers whose names have been widely reported cannot subsequently be deployed across the full range of the services' work, and thus years of training and experience needed to reach the required level of competency can quickly be ruined. And the more a name is repeated across the media, the greater the damage. The net result of such disclosures is to deny Britain valuable intelligence about hostile intent or capabilities. It is an undeniable fact that attempts to breach Secret Service secrecy harm the people directly involved (whether or not they are Secret Service members) and ultimately they can - and often do - harm us all: that includes you and me. They ruin lives and for some lead to injury or death. For the Secret Services, secrecy is not some outdated fetish; it is the key enabler in the job they do; quite simply they cannot protect us without it.

We can draw three important deductions from all these points. Firstly, that a degree of secrecy – qualified certainly by time, subject matter, detail and oversight - is indispensable in preserving security. Secondly, that there are practical limits to how much information, and for how long, any government can keep secret. And thirdly, keeping secrets in the modern World depends on consensus and shared responsibility. The release of a highly classified secret may not damage security if it can be found only on an obscure website or journal which few if any read; de facto it remains buried. The problem for security begins when it becomes widely available in the public domain and difficult to ignore even for the most casual browser. When that happens there is no telling who might find it or to what use it might be put. And in deciding whether a piece of information is or is not widely available in the public

domain, it is the media that plays the decisive role. It is ultimately they who will judge whether or not, and how widely, information is published or broadcast, and in reaching that decision they face balancing their own rights and interests against their wider societal duties and obligations.

This is the key premise that underpins the UK's Defence Advisory (DA) Notice system. Unique to Great Britain, this system emerged at the end of the Cold War from the long established 'D Notice' system, which was widely seen as a form of government censorship. The present DA Notice system was shaped to meet the very different conditions already emerging in the early 1990s, and was from the outset based on consensus and shared responsibility between government and the national media for the disclosure of national security information. The system is overseen by the Defence Press and Broadcasting Advisory Committee or DPBAC – an independent body with a joint membership of 5 very senior civil servants and 13 leading members of the UK media. All government departments concerned with national security are represented, and the DPBAC media members represent virtually all areas of the UK media. These include the BBC, ITV, ITN, Sky TV, the Periodical Publishers Association, the Newspaper Publishers Association, the Newspaper Society, the Press Association and the Scottish Daily Newspaper Society. The (book) Publishers Association have so far chosen not to be represented on the Committee, but their members nevertheless use the DA-Notice system. Links have also been established with the UK Internet Service Providers Association.

The code endorsed by the DPBAC is set down in five standing DA Notices which define the areas that the Committee considers to be at the core of national security. And that is their limit; they do not extend to any other sensitive areas which a government might wish to keep secret, such as internal policy disputes, waste, vice, scandal, corruption, failures in military discipline and the like. They are not orders, but purely requests, ones which are framed broadly to allow scope for sensible interpretation.

DA Notice 1 deals with UK armed forces' operations. It asks journalists and editors to seek advice from the Committee's secretariat before publishing or broadcasting details of current or future operations, methods, tactics and contingency planning, to meet particular hostile situations and to counter threats of terrorist attacks, units' readiness states and operational capability, units' operational movements. An example of this was when in December 2004 UK journalists were asked not to publish details of the timing or route of the withdrawal in Iraq of the British Army's Black Watch battle-group from Baghdad to Basra. Such information would have been a gift to the insurgents hoping to stage an ambush.

DA notice No 1 also covers particulars of current or projected tactics, trials, techniques and training as well as details of defensive or counter-terrorist measures taken by individual installations or units to protect themselves against terrorists or other threats. As you will appreciate, the release of details in any of these areas could allow an enemy to devise effective

counters that would lead directly and quickly to the death and injury of British troops and perhaps to operational failure.

DA Notice No 2 asks that, before a journalist or editor discloses highly classified information about certain types of nuclear and non-nuclear defence equipment, he or she should first seek advice. Clearly, the release of highly classified nuclear weapon information could jeopardise the safety and security of the UK's nuclear forces, reduce their deterrent value and enable others to develop such weapons in breach of the British Government's non-proliferation obligations and ultimate disarmament objectives.

DA Notice No 2 also asks journalists to seek advice before disclosing highly classified details on certain non-nuclear defence and counter-terrorist equipment, particularly design details, technical specifications, performance figures, operational capabilities and areas of vulnerability to counter-measures. Again the rationale behind this is clear. The disclosure of such information could enable potential enemies or terrorists to devise effective counter-measures more quickly, to speed up the development of their own weapons and equipment and to alter their operating methods so that attacks which might otherwise have been frustrated could prove successful. And all that could lead quickly and directly to increased British civilian and military casualties and potentially to operational failure.

DA Notice No 3 asks the UK media not to publish or broadcast without prior consultation details of the British Government's highly classified codes and ciphers, related data protection measures and communication facilities, or those of NATO or other allies. It also requests advice to be sought before

disclosing, or elaborating on, information published at home or overseas about UK official codes and ciphers or their potential vulnerability. The rationale behind this is again obvious. Compromised codes and ciphers put at risk the classified information which they are created to protect, threatening security and indirectly lives.

DA Notice No 4 asks that care should be taken not to publish home details of individuals likely to be targeted by terrorists, without first seeking advice. This Notice also asks the British media to seek prior advice before publishing or broadcasting information of value to hostile persons or governments about key facilities and installations. This includes high security military sites, intelligence facilities, sites of crisis headquarters and communications facilities for use by government or NATO in time of crisis, and serious vulnerabilities of a long-term nature identified in the Critical National Infrastructure (CNI) which if directly attacked could cause major widespread disruption and/or loss of life

The final DA Notice, No 5, asks the UK media to seek advice before revealing the identities of staff from the intelligence and security services, others engaged on sensitive counter-terrorist operations, including the Special Forces, and those who are likely targets for attack are at real risk from terrorists. I mentioned earlier the importance of not disclosing secret service identities, and even higher levels of secrecy are needed to protect security and intelligence operations. Publicity about a secret operation which is in train finishes it. Publicity given even to an operation which has been completed, whether successfully or not, may well deny the opportunity for further exploitation of a potentially unique capability against other hostile or illegal

activity. Even inaccurate speculation about the source of information on certain issues can put intelligence operations (and, in the worst cases, lives at risk) and/or lead to the loss of vital national security information.

Please note that these DA Notices have been agreed by representatives of the UK government and media, are published in full and can be accessed by the public on the DPBAC's website: www.dnotice.org.uk. They are framed to permit sensible interpretation and negotiation between journalists, authors and editors on the one hand, and the DPBAC Secretary on the other. They act as a societal agreement between the UK government and media to share responsibility for the disclosure of national security information, one which upholds the media's right to report in the public interest but recognises it has an obligation to ensure that the public is not damaged as a result.

The two key supporting pillars of this very British arrangement are confidentiality and consent. Journalist and editors must have confidence that when they seek DA Notice advice it will not be used against them or their story passed to competitors. Without that assurance they would cease to seek advice and the system would collapse. It was this reality, and the feeling that the Committee must retain its independent status, that led the DPBAC to conclude (apparently paradoxically) that they should not seek to become subject to the UK Freedom of Information Act 2000 or the Freedom of Information Act Scotland (2002). The Committee ensures full transparency about its policy and the debates that lead to its formulation – inter alia - by the publication in full of the minutes of its meetings on its website. But the continuing effectiveness of the system relies on individual casework, and the

advice offered by the Committee's Secretariat to government officials and to members of the media and public remaining strictly private.

The second of the system's supporting pillars is that advice offered under the system does not have to be accepted. It is a purely voluntary code, unsupported by any form of legal sanction. A journalist who seeks DA Notice advice on his/her story, is perfectly at liberty not to accept that advice, either in whole or in part. Even if advised against it, he or she is fully entitled to publish or broadcast the information concerned if, for example, he/she believes that the case made for not publishing is weak, or if a very important principle is at stake. In effect the system is meant to act as a safety net for journalists and editors; something which does not gag them but helps to ensure that they do not inadvertently damage national security.

As you will already have guessed there are many problems with this system. The voluntary nature of the DA Notice system exposes it as much to criticism from hard-liners who would prefer more draconian sanctions for perceived security breaches, as to civil libertarians who see in it a disguised form of censorship and a way of seducing the free press. It is also a very tricky system to manage. The issues involved are rarely clear cut, and usually highly subjective. They include many things about which reasonable people could disagree. Also, the media agencies who take a responsible position and seek DA Notice advice often feel disadvantaged in comparison with those who don't and who publish or broadcast damaging information regardless of the consequences. In perhaps the World's most fiercely competitive business,

one in which the British media see themselves as leading players, this is very important. Associated with this, the DA Notice system is British-only, whereas news and information services and threats to security are already overwhelmingly international in their character. It also relies on consultation in an era of real-time and world-wide TV news broadcasts that can instantly put information widely into the public domain that cuts right across the code.

All of these areas of challenge can only increase in the future. As the electronic media becomes ever more technically integrated, as search engines become ever faster, more discriminating and more powerful, as people are able to access World-wide news through a growing number of gadgets and as media competition becomes ever more fierce, it will become increasingly difficult to argue that after its release that a piece of information is not automatically widely available in the public domain and easily accessed.

Does all of this suggest that the British DA Notice system, already imperfect, is likely to decline in effectiveness in the future? Perhaps so; we shall have to wait and see. But even if it does decline, would that be a good enough reason for abandoning a system which continues to contribute to our security? What are the alternatives to it? Seeking greater secrecy through more stringent and intrusive legislation? I know of no one who wants that; and anyway, for all the reasons mentioned earlier, Britain already has what most people see as the maximum practical level of secrecy in the existing conditions. Unless the security situation worsens markedly, the public is unlikely to support the loss of freedom which a legal resort to greater secrecy would impose. The only

other alternative to that would be a free-for-all in which British journalists, denied the benefits of authoritative advice, would run the risk of inadvertently publishing or broadcasting information that would cause the death or injury of British troops or civilians. I know of no British journalist who wishes to be responsible for that either.

Someone once said that democracy is the worst form of government, with the exception of all the others. Similarly, it could be said that the DA Notice system is the worst way of providing national security media support, except for the alternatives. Secrecy like security is never absolute; it is always limited and relative. The DA system accepts that reality and works within it. In any case, Secrecy is just one of many elements in any security structure, and it has to be kept in balance with the others; in terms of national security this includes most notably public and media consent. Despite its limitations, the DA Notice system continues to be relevant and make a contribution. It has delivered a great deal in the protection of our national security simply because it accepts that media-government relations in this area at least must be based on a partnership rather being automatically adversarial.

At a time when a depressingly wide spectrum of groups regard the serialised mass slaughter of innocent individuals as a perfectly acceptable policy instrument, difficult balances have to be struck. One of those balances is that between security (in its widest interpretation) and secrecy. The most precious of all human rights is the right to life, and to preserve that today some information has to be kept secret. To ensure that that secrecy is not exploited

for purposes other than preserving national security, it is far better that sensible people enter into a dialogue within defined boundaries as to what should or should not be placed, or at least widely repeated, in the public domain. This avoids wholesale recourse to the law courts, or – even worse - more restrictive laws formally extending the bounds of official secrecy. Such a dialogue fosters collective responsibility for something of key importance to us all, and it upholds the absolute right of the media to breach the established guidelines without the threat of legal sanction if they judge at any time that the arrangement is being exploited or that a crucial principle is being risked.

I would like to finish with two true stories about the Duke of Wellington – the man who defeated Napoleon at the Battle of Waterloo. The first was in Wellington's early days as a British commander in India. He was asked by a local ruler to disclose a particular piece of intelligence in exchange for a large bribe, a common enough transaction in those imperfect times. The Duke looked furtively over his shoulder and, coming closer, asked if the ruler could keep a secret. The ruler's eyes lit up as he answered 'Yes, of course I can'. The Duke, with that cold aloofness for which he was to become so famous, replied in turn: 'Well, so can I!' Indeed Wellington could keep secrets and did so throughout his life. When asked by Lord Uxbridge (his second-in-command) immediately before the battle of Waterloo what his plans were, Wellington simply replied 'To beat the French'. He followed this with an aside that 'If I thought my hair knew what my brain was thinking I would shave it off immediately'. In today's World we don't need to go to those lengths, but we should surely recognise that a degree of secrecy is indispensable for security.

In trying to strike the right balance between ‘secrecy and security’ we can safely set aside Orwell’s Animal Farm slogan of ‘4 legs good, 2 legs bad’, as we can also its successor ‘4 legs good, 2 legs better’. Instead we should recognise that ‘4 legs good, 2 legs also good’ does apply here, at least at certain times, in certain carefully defined and broadly endorsed areas and provided it is applied with common sense and moderation and tempered with proper instruments of oversight and public accountability.

4th
International Conference of
Information Commissioners
MANCHESTER 2006

The Presidential Executive Order on the Freedom of Information Act

Daniel J Metcalfe, Director, Office of Information and Privacy, United States Department of Justice

I am very honoured to be here representing the United States and to share the US experience of the Freedom of Information Act with you. I cannot hope to match the eloquence of the three speakers earlier this morning that we all heard, nor do I have a Powerpoint presentation, graphics or otherwise to speak to you about or from, but I can at the outset fairly make some claim to paternalism, both on behalf of the United States and myself, with respect to the literal explosion of openness in government - Freedom of Information, transparency – use whatever label you would like. Regimes are largely by law, but not entirely, in the case of Argentina, explosions of those regimes just in relatively recent years.

Now I say paternalistic but I should acknowledge that Sweden is the grandfather or perhaps even the great grandfather of openness of government, because Sweden began that tradition, as many of you heard, in

1766. Little did we know in the United States that we were celebrating the two hundredth anniversary of that tradition when our Law was enacted in 1966. And when I began my current position, after having been a trial attorney for several years, in 1981, there were but a handful, a literal handful of nations of the world that had any true openness regime whatsoever, the United States being not the longest term but certainly the most relatively mature at that time. And I say paternalistic feeling because beginning in 1981 beginning with my colleague Dick Huff, who some of you have met at Cape Town and Cancun – he and I were co-directors of our office for many, many years in a somewhat unique relationship within the Federal Government system, we have met with literally hundreds of delegations of what we call foreign visitors. We have described the operation of our Law to encourage first the development and then the implementation of like laws and systems overseas and what we have said time and time again is “Learn from our mistakes”, because certainly in the United States we have had our growing pains of Freedom of Information Act tradition.

What I’d like to do is just sort of set the stage briefly this morning, talking about the basics of Freedom of Information in the United States and then to talk about the latest most significant development we have had by far, certainly emanating out of the Executive Branch of our Three Branch System of government and that is an Executive Order, a special presidential order issued to promote, encourage, foster Freedom of Information, in just December of last year. Our Law as I mentioned was enacted on our Independence Day July 4th 1966. It took effect a year later, July 5th actually

1967, but it followed a tradition of 20 years basically that moved toward openness. We had an Administrative Procedure Act, an Act enacted shortly after World War Two in 1946 and then 10 years after that in 1956 our Congress started very seriously considering whether there should be a Federal Freedom of Information Act and you can tell that that took about 10 years. That's not quite as long as it took in Japan which was closer to 20 and I say that not in a pejorative way or not because there is no-one from Japan here, but it took longer in some nations, and much longer in other nations thereafter. But it took a full ten years of legislative consideration, 1946 that General Administrative Act, 1956 we began legislative consideration, 1966 we enacted the FOIA – you're beginning to see a pattern perhaps?

Then the FOIA was heavily amended in 1976 and amended again in 1986, amended again in 1996. A decade ago after the 1996 amendments which we call our EFOIA our Electronic FOIA Amendments as I would describe this pattern people would say well what is next for the year 2006? I said that of course that was the year that I would become eligible for retirement so that would continue the pattern in that way. Actually, last year we had serious legislative proposals introduced in the first session of our current Congress to further amend the Freedom of Information Act, including for the first time to perhaps include the Ombudsman concept on behalf of FOIA requesters and that's something that has led to further administrative action since then. So that ten year pattern has held pretty firmly and actually I lied when I said 1976 because although our Act *was* amended in respect of one of our exemptions in 1976, in fact our major amendment, probably the biggest of all between the

70s the 80s and the 90s occurred not in 1976 within that pattern but rather in 1974, two years earlier I would say because -- has anyone ever heard of the scandal in the United States called Watergate at the end of President Nixon's Term? What basically happened was that in the summer of 1974 when President Nixon promptly resigned in the midst of what were about to be impeachment proceedings they had started, but they hadn't reached fruition, they were a whole bunch of legislative staffers who were literally all dressed up with no place to go, one of whom included the young Hilary Rodham, later Clinton who was on the hill and what happened in 1974 is that Congress having this build up of resource in anticipation of the full impeachment and trial of President Nixon decided that as they had some time on their hands they would amend the FOIA and enact the Privacy Act of 1974 and one might think that Congress did the two at the same time so surely they fit together like hand in glove because they were contemporaneously enacted. The answer is no, our Privacy Act and our FOIA are put together like this, that is to say not smoothly at all, somewhat rough about the edges. So I can sympathise with Richard [*Thomas*] when Richard has both parts of that responsibility conjoined within his office - I know the difficulty of having a smooth interface between the two, especially in our legal structure.

So just to continue briefly to set the stage, in the United States we are now approaching our 40th Anniversary of the enactment of the Law and we'll celebrate that in July. We will probably celebrate the enactment more than the implementation because again that pattern of the six years or the years ending in 6, we are at this point in a very mature stage of our existence. One

could even say that our FOIA ["*Foy-yer*"] (and by the way I always pronounce it that way. In the States we always say, "It's good FOIA" or, "Go out and have a drink in the FOIA foyer out there" perhaps), our FOIA is now at the point where I think it has reached middle age and we have now more than 4 million requests in the last accounting for fiscal year 2004. We spend more than 350 million dollars I think it's fair to say that it's going to be in the next accounting the aggregate number will be over 200 million pounds per year in processing those millions and millions of requests. Now how is that done within the Federal Executive Branch of the United States Government? We have 90 Federal Agencies, 15 Departments – the newest of the group the 15th being our Department of Homeland Security that was created in 2003 after our Homeland Security Act of 2002 which of course was in the wake of the terrorist attacks of September 11th 2001 – so 15 Departments, of which the Department of Justice is one, 75 other Agencies. And among those 90 Agencies of the Executive Branch they process those 4 million plus records on a decentralised basis, in other words each Agency handles its own and then within Agencies, especially the larger Agencies or Departments like the Department of Justice, we are decentralised again. The Department of Justice is comprised of 40 distinct components, one being the Attorney General's Office, one being the FBI, the Bureau of Prisons, the Criminal Division and the like. My Office is sort of medium sized in the relation of those, we're 46 people and we're one of those components.

So what we do is we have to give guidance to all of those 90 Federal Agencies. We guide them on how to interpret and apply the Freedom of

Information Act. We do an enormous amount of training. We have what we call our FOIA hotline and we receive more than 3000 calls per year, we produce a lot of written guidance. As a matter of fact we started years ago with our standard guidance vehicle, which we used to call our 'Short Guide to the FOIA'. Well, we now have had almost 6000 cases decided since 1967 and truly a very relatively few of them were within the first 7 or 8 years so it's backloaded in time if you will, our Short Guide to the FOIA is now 885 single spaced 14 inch pages reduced down to here with more than 35 hundred footnotes. And this will be something that we revise every two years. We will have a new version in 2006 that will be silver in colour because of the silver anniversary of my office which was formed in 1981.

And what we have to do is guide all the Agencies in what to do, how to apply the Act, how to interpret the Act. We develop policy on the contours of Exemptions, because believe me, as time goes by those initial questions become even more and more refined as you get down to the little intricacies of exemptions versus disclosure and where to draw fine lines. Those arteries become veins and those veins become capillaries of interpretation with the passage of time. We have certainly seen that within the United States, and I have seen that from my own experience - I've been doing this since 1981.

I mentioned litigation with all those cases – certainly that's a big part of shaping our Law, but at the bottom, the authority of the Department of Justice is sort of a combination of things that I have heard at this programme so far. We have moral suasion that we use (I heard that phrase used), we also have

a hammer (I heard that phrase used) in that if an Agency does not follow our advice and does the wrong thing and withholds too much information, all the requester has to do is bring a lawsuit which doesn't cost that much in the United States. We have a lot of prisoners in jail who bring lawsuits at the drop of a hat we- sometimes say that when they go there they get the striped suit and the tin cup and then they get the FOIA request form, all as a standard package that comes together as a piece! It doesn't cost that much, a lot of them pursue it on what we call a "pro se" basis and in those law suits, if the Agency has done wrong shall we say, the Department of Justice with very limited exception of Independent Regulatory Agency like the Securities and Exchange Commission, with very limited exception, the Department of Justice has the authority to decide whether to defend in Court or not.

So ultimately at bottom, behind all the guidance we give, telling Agencies and admonishing them and sometimes in a very hortatory fashion as to what to do and how to do it, at bottom they know that if they don't do it right and they're sued, we can refuse to defend. And as you might imagine, with that sort of a sanction or threat or a 'stick' it's not the use of it – you don't have to use it that often – it's the potential use of it that makes a difference, and it really does have a big effect.

I would say that overall, our exemptions, and we have nine basic ones and then law enforcement ones divided into sub-parts, there are five most significant areas overall of exemption activity in deciding whether information should be withheld from the public. The first is privacy and it should not

surprise you to hear me say that. The privacy principle or tradition in the United States is quite strong. I cannot go so far as to say that it's as strong as I think I heard the phrase it was Andrew who said "Privacy secrecy". That seems to me to be a very strong phrase. We are not quite as far as that connotes to the average reader or listener, but very, very strong privacy, so much so that in our most recent Supreme Court Decision, we have finally officially firmly enshrined the principle that I call 'survivor privacy', and by that I mean to say that if an individual is deceased, as a general rule that privacy dies with that person under our Law. But, in exceptional cases, usually where the records or the information in the records involves something incidental to death, autopsy report for example, or in the case that went to the Supreme Court, it was death scene photographs of former Deputy White House Counsel Vincent Foster, who committed suicide in July 1993 just 6 months after the beginning of the Clinton administration. And let me tell you, for those of us who lived through the beginning of the Clinton administration, which Vince sadly did not, those 6 months seemed like about three years, just because there was so much being done right at the very beginning. He sadly suffered from depression, committed suicide, there were photographs taken of his body in Fort Marcy Park in Virginia just across the Potomac River from Washington DC and there are a lot of people who to this day think that it was part of a conspiracy, that he was murdered, that his body was moved, and that so on and so forth. We protected those photographs to protect the sensitivities, the sensibilities, the quiet enjoyment if you will of his wife and then minor children so that they would not have to walk into their high school classroom where there was a television in the corner and see suddenly a

death scene photograph of their father because it came on the news perhaps. And that was enshrined just recently. I felt personally about it because the very concept of survivor privacy is something that I originated on my desk literally in April of 1978 when I had the responsibility for defending a law suit involving records on the assassination of Martin Luther King, and I withheld some FBI information on a survivor privacy basis and then many years later that was enshrined by our Supreme Court.

Privacy is big, national security, certainly that's no surprise to any of you. National security tends to blend or blur into homeland security – that is the new buzz word in the United States after the attacks of 2001. Homeland security. Business confidentiality – some people say that the business of the United States is business. That's an old fashioned phrase, but I think it's fair to say that our experience under exemption 4 and business related requests fits that phrase. That was one of the major miscalculations of our Congress – no-one ever envisioned in our Congress truly had the slightest idea in the 1960s that our FOIA would become a means of industrial espionage and on a very much tit for tat basis if that's a viable phrase, where one business seeks information held by the government and then the other business retaliates back and forth. It has even bred what we call reverse FOIA litigation where business information comes to the government and instead of a regular FOIA requester who might go to Court and say, "Your Honour, disclose their record to me, make them disclose their record to me". The business goes into Court and says, "Your Honour, order them not to disclose their record to the FOIA requester." Hence reverse FOIA cases – we have many, many of those,

involving information that is submitted to Federal Agencies who regulate businesses in one way or another. We have a highly regulatory society, a highly regulatory approach in our system of federal law and also with respect to procurement. And I've heard mention here more than once contracts and the issue of disclosure of contract information, both awarded contracts and maybe un-awarded contracts where they merely were bidders and one competitor wants to learn what the other one bid for the next time around. That's the third big area. The fourth I would call under our exemption 5, we have three major privileges, attorney/client, attorney/work product and I have heard reference of something akin to that here, but the big one here is what we call the deliberate/process privilege and I think it was Nico this morning who gave a very good articulation of it and called it 'the space to think' if I remember correctly. That's the same thing – something which protects the deliberation. There is a lot of controversy over that within our system largely because there is room for discretionary judgement to be exercised, and one thing that I've not heard discussed here today is the concept of discretionary disclosure, by that I mean to say that even though something does fall within an exemption, an Agency still could, as a matter of administrative discretion say "You know, it's exempt, we're legally entitled to withhold it, but we're going to release it anyway". That's something we did as a matter of policy during the Clinton years. I think that the reason I've not heard that so much I suspect is because largely in European systems the counterpart to that is what I would call the 'public interest override'. There it's significant, because the public interest override determines whether something *is* exempt to begin with, here I'm talking about whether something that perhaps involves a

deliberative process *is* exempt but the Agency might disclose it as a matter of discretion or largesse nevertheless.

The final area is law enforcement information and I haven't heard that much discussion of that in the last two days here but that is big business in the United States especially I guess in the Department of Justice because our FBI is involved in so much activity by the DEA, Drug Enforcement Administration as well. That too, I should tell you, tends to blend or blur into the homeland security area, such that right now it is sometimes difficult to discern, and a lot of people outside of government express frustration about this, but it's sometimes difficult to discern where national security ends, law enforcement begins or homeland security begins or ends. On a continuum we have all three together, blurring together since September 2001.

Now what are the big areas of controversy in the US system? I've heard a lot of talk about backlogs, and I would have to put backlogs as number one in our system. Ever since the beginning there have been backlogs government-wide, across the board, mostly of the larger Agencies that have to deal with the especially complex records – law enforcement records, intelligence records, sometimes business records but that's really a far distant third. Intelligence and law enforcement, our State Department, our Justice Department, Homeland Security, our Intelligence Agencies, the CIA certainly, that's where the backlogs have been the biggest problems over the years. I will have to respectfully disagree with Lord Falconer because yesterday he said he would like to see 100% compliance. I'm here to tell you, based on US

experience, that that will never ever happen. That is not even a reasonable aspiration, because if 100% compliance means that requests will be responded to within the same 20 working day period that we now have under our 1996 amendments, you can have an Agency that is perfectly fine, perfectly in good shape, then all of a sudden along comes a request that throws everything out of whack. One of the first cases that I defended in Court in 1977 was a case involving three quarters of a million pages of Watergate investigatory records. Well I'm here to tell you that at that time we spent many, many minutes, the Agencies did, processing each of those pages. There is no way that even in an Agency that was perfectly all tickety boo at that time, everything was fine and set to begin with, could process something like that within 20 working days, or even 200 working days, possibly not even within 2000 working days. So even if you have an Agency that's all lined up perfectly it's unrealistic to expect that you will have 100% compliance. It's an aspiration, but it's nothing more than that I suggest to you.

Second big area of controversy over the years – fees - and I think that that will become a growing area of controversy perhaps in the UK. It might take some legislative amendment to change the current threshold for fees, but over the years, we have problems with fees, with requesters saying not just that the fees were too high or unwarranted in particular respects for duplication or for copying, but rather that they should not have to pay fees. On a public interest fee waiver basis, or more categorically because the news media representatives or representatives of academic insitutions, that has been and always will be a controversial area under our Law. And then thirdly of course

there's the application of exemptions, withholding of information, and that ties with the five things that I outlined earlier.

Over the years, we have in our policy role of the Department of Justice set the tone for FOIA administration as we have gone from presumably more conservative republican administration, I go back to the first Reagan administration in this job, the first Nixon administration originally with the Department, to more liberal democratic administrations, with the idea that the Republicans are less favourable towards openness and the democrats are more inclined towards openness, we set the policy with an Attorney General Memorandum. There was one issued in 1977 in the Carter administration, one again in 1981, and then in 1993 we had the most significant one of all and that was issued by Janet Reno when she was Attorney General for eight years under President Clinton. It was accompanied by a one page policy memo signed by President Clinton. What happened was that I drafted several pages, it went to the White House, Clinton liked it so much he took the first page for himself. He was President, he was entitled to do that, that's OK, and then Janet got the remainder. The two of them were issued in October 1993. They fostered and promoted discretionary disclosure. Then we had a replacement one that was issued by Attorney General Ashcroft at the beginning of the current Bush administration. It was issued a month and a day after 9/11 and a lot of people said it was just a reaction to 9/11 but they have a problem with that because I can look them in the eye and say no, I changed only one word after 9/11. It's just coincidental that it was issued at

that time – it was in the works long, long before then. That does change policy back a little bit in the other direction.

Now, what's happened most recently with the Executive Order? This is something unlike anything we have ever had before. We've had these policy statements from the Attorney General, even that one add on from President Clinton in 1993, but an Executive Order in our system of Law, that has a very distinct and heavy force of law. I can stand in front of those 90 Federal Agencies with my moral suasion and my hortatory approach and my stick in my pocket about not defending them in Court and I can do this all day long. But at bottom, I also play an ombudsman role believe it or not in some respects, but at bottom, an Agency can decline, can refuse to do what I am saying. That is really the fundamental reality. It doesn't happen often but it can happen. But when you have a President who says in an Executive Order "Thou shalt do this", well that has to be done without any question.

What this Executive Order does, is that it tells all Agencies two things basically, one that we have a more general openness policy of being friendly with FOIA requesters, customer friendly you might say, helping them to keep track of FOIA requests that might be caught up in backlogs that are sometimes perceived by FOIA requesters almost as black holes with the passage of so much time, and it also tells all Agencies no matter where they stand with respect to backlogs and anything else, that they have to improve, that they have to do something to improve their processing. Every last Agency of the Federal Government down to what we call the little micro

agencies. If we go up to 90, when you get into the high 80s some of them are so small they barely even know they are Federal Agencies – the American Battle Monuments Commission, and they may get a FOIA request or two per year. All of them now have to have Chief FOIA Officers who are political non-career employees. They have to have FOIA requester service centres, they have to have FOIA public liaisons which is a form of Ombudsman perhaps not truly, but something certainly akin to that at least a little bit. They have to establish these positions and under strict timetables this year they have to through their FOIA officers and their FOIA liaisons review all of their FOIA operations, conduct that review, finish that review by June 14th which is coming up quickly darn soon, and they have to come up with improvement plans, very concrete improvement plans. And that is something that has hit our system by storm, because it's very specific, it's not a concept or an idea or a policy with loose fuzzy edges, it's very, very concrete. They have to produce these plans. And I have gathered our Agencies together in FOIA officer conferences, sitting them down and again admonishing them about how they have to follow this requirement and that they have to conduct their reviews I have given them a lot of suggestions, I have published guidance to guide them toward that in many different respects and what's now happening after the fourth or fifth session that we're going to be having very soon, is that they are putting the finishing touches on these improvement plans.

Now at the Department of Justice, it's a three level enterprise, especially in my office, because we are a) guiding all 90 Federal Agencies, b) I have responsibility for all 40 Department of Justice components, because when we

have FOIA requests we have 55,000 of them a year at the Department of Justice then 3,000 administrative appeals, I adjudicate those 3,000 administrative appeals per year, which is more than any other Agency, and have responsibility to do this for each of our 40 components. And then, within my own component, we also process what we call initial requests, beyond the administrative appeals, because we have that two level system of review, for the Attorney General, Deputy Attorney General, Associate and five other leadership Offices including my own Office, so in our Office, we have three levels of responsibility, to get all the Agencies government-wide to do this to have all the components of the Department of Justice to do this and then in my own office we have responsibility for 8 of those 40 components. And we are obliged as best we can to encourage Agencies, to urge them to improve things as much as they can.

Now what are the big areas that they have to look at? The first, consistent with what I said about the big areas of controversy, is backlogs. Backlogs again have always been and I do believe even after this current review and improvement period will always be a major if not *the* major source of frustration and controversy within our system for FOIA, not every Agency to be sure, but certainly the big ones. Backlogs are a major problem. This Executive Order says: Agencies have to come up with plans to eliminate or reduce backlogs. It is astonishing to many people that it has the word eliminate in there. Frankly I will reveal something about our own deliberative process when I say there might have been some of us who attempted to eliminate the word eliminate, for the same reason that I would tell Lord

Falconer that it is unrealistic to aspire to 100%. Eliminate or reduce – a very heavy message. That has got to be a part of every Agency's plan that has a backlog of pending requests and that means more than 20 working days, it includes the big request that may come in every now and again. So we have said that that is one of three major areas that you have to focus on.

Another one is what I would call proactive or affirmative disclosure of information and I've heard mention of that at least once or twice and that flows also from the electronic evolution that we now have a point at which the web and websites are a very heavy part of FOIA administration. Agencies can simply place information out there affirmatively or proactively, and there is a slight distinction in our system of law. Affirmativeness or proactivity can reduce the need to make a FOIA request to begin with. The slight distinction by the way is that when I use the phrase affirmative disclosure, that's a legal requirement.

In our Law we have an obligation, especially after the Law was amended in 1996. To put some information up on the web by law, in other words by legal compulsion, it has to be up there, so we have to meet that obligation in order to do that. Proactive disclosure is more akin to what I said before when I talked about discretionary action, where an Agency is not legally required to do it but boy you know it would make a lot of sense to do it. If they think a little bit, they say you know, we're not required to put this up, but if we do maybe that can cut down on the need to make FOIA requests. Maybe it could

be good for us, maybe it could be good for the potential FOIA requester – good all around. It is a very heavy part of what we are looking at.

Now the third area I am going to use as a segue to get into another emerging topic in US Law. The third area has to do with what is now being called and it's in the last year that the name has really been coined – 'Pseudo-Secrecy'. Pseudo-Secrecy is a relatively new term that in a nutshell describes a system of safeguarding information (notice I said safeguarding, not withholding), for use of safeguarding labels independent of whether there is ever an issue of FOIA disclosure.

In our own classification system, national security classification system, which has existed since the Truman administration, there is a duality to classifying a record, this is on national security grounds mind you. The duality is this: if I'm in an intelligence Agency and I'm a classification officer and I take that action, on a given day I will classify that record, it will have markings, a safeguarding label if you will, and if no-one ever makes a FOIA request for that, that will be the end of the story. That label will guide or govern how the information is maintained by the Agency, how it might be shared within or without the Agency, it has nothing to do with public disclosure per se. If it becomes subject to a FOIA request, then if it's classified our first exemption applies, and it's pretty darn categorical. It's not inviolate, but it's pretty darn categorical. That's a standard situation.

What I'm talking about are safeguarding labels that are beyond things that are classified on national security grounds, things that are just deemed to be sensitive by the Agency. Now what do I mean by the word sensitive? I don't know, because that's sort of a loose or amorphous term, and when Agencies apply those labels such as For Official Use Only, if you ask them what they mean by that they don't really know. Does that mean it is exempt under the FOIA? Well maybe, maybe not. There is an imprecision there that to those outside of the government is very, very increasingly troubling, especially since 9/11 because if we talk about nuclear proliferation, that word proliferation is used a lot, but we have had safeguarding label proliferation since 9/11 – FOUO, SBU (Sensitive but Unclassified Information), we now have reportedly as many safeguarding labels in the United States system as there are nations of the world that now have a FOIA, about 60. Some of them absolutely correlate to FOIA exemptions, classification as I have described, one on one 100% correlation.

We have things that we call Exemption 3 Statutes where Congress in a distinct Statute "Thou shalt not disclose". Well when Congress says that, when we get a FOIA request we apply our third exemption, case closed. We don't have to violate a Statutory Prohibition on disclosure to comply with a FOIA request. You will have complete identity between the safeguarding label and the FOIA exemption applicability. But in the vast majority of cases, especially recently since 9/11 with the proliferation, we have had imprecision and a lot of misunderstanding within Agencies. And if you read the popular press of the United States, the word secrecy is thrown around in a very, very

broad way and part of my job when I speak to media groups and public groups is to dissect that. I say “Friends, countrymen, I come not to praise secrecy…”, I come to dissect it for you, because I’m telling you that the word secrecy could mean something as relatively simple as you put a label on it, and maybe it will be exempt under the FOIA maybe not, we could be withdrawing it from the web out of a post 9/11 concern but it wasn’t required by law to be up there to begin with - that can be called secrecy. I would suggest that true secrecy is only when information is withheld from the public in the face of a public access demand, in our system a FOIA request. That’s where the rubber meets the road if you will, that is true secrecy.

And when we have something that’s labelled “For Official Use Only”, FOUO for short, well that doesn’t necessarily equate to a FOIA exemption. Will it give the FOIA officer some pause when processing that record in response to a FOIA request? You bet – that’s part of the labelling dynamic to begin with, in order to do that. However, it doesn’t translate to FOIA exemption. We have to make sure that we explain that to FOIA officers so we can go out to the public and say wait a minute, you may have a lot that you were rightfully concerned about with respect to government secrecy, you may be worried that we are expanding our exemption 2 in a post 9/11 sense, looking at things through a post 9/11 lens. You may think that we’re having more and more exemption 3 statutes – that’s legitimate. Reasonable people can disagree. But if you think that we have more secrecy in a disclosure sense just because of a safeguarding label, the answer is no, that is an imprecise analysis. And for that reason, this is the third of the three big areas that we talk to Agencies

about to have them put in their plans. We had 27 suggested areas for improvement, one of which was for Agencies to go to all their people and make sure that those who process FOIA requests knew that it was OK to pause if they saw a safeguarding label but that pause and that careful analysis does not necessarily mean it's exempt. Only a FOIA exemption can properly stand as a legal barrier to disclosure in the face of a FOIA request. And sometimes I even try to get their attention, especially when I talk to our Defence Department where FOUO is a big, big label. I say FOUO is 'Phooey' when it comes to FOIA. It does not necessarily mean it's exempt. Maybe yes, maybe more than half the case, maybe most of the information, not necessarily all of it. But in that situation it's not necessarily exempt. So that is one of the three of the 27 areas that we have encouraged all Agencies to look at in connection with their plans.

Now the next step, when we all come out with our plans on June 14th, is for Agencies to start implementing them, and after that, the Attorney General has the obligation to file a report to the President on how Agencies have been doing in their reviews in the creation of their plans. And I have been able to use that stick with Agencies and say, "You know if you're an Agency with a backlog, and you don't have backlog reduction, forget elimination perhaps but at least put reduction in your plan because you can imagine that the Attorney General come October 14th is going to be pointing to you as the one Agency that is sticking out like a sore thumb as it will, and you won't want Congress on your back like that and you won't want public interest groups to be looking at you in that way.

Then after that we have another obligation. February 1, all Agencies have to report on their implementation. And then again on February 1 2008 they have to report on their implementation. Again. So that will cover the next two annual reporting cycles. And I think that at the end of all of that, even if one were to be cynical about the success of Agencies in developing their plans and implementing their plans, even if one were to take the most cynical view that's possible, and there are people in our system in our NGOs who are inclined to take the most cynical approach and frankly that cynicism is something which is born of experience, very concrete experience that they have, so I'm not trying to denigrate that, but even if you take that cynical approach, I think that as a minimum, what will be happening in the United States is a very firmly renewed commitment, a refreshed commitment to the administration of the FOIA, just in time for our 40th Anniversary. Whether you count that as the 40th Anniversary of the Enactment in July of this year, or the 40th Anniversary of Implementation in July of 2007, at a minimum, you will see that FOIA in its middle age in the United States is getting sort of a booster shot in a very pro-requester direction.

And maybe if that works well, we won't need to have the 2006 amendments and there are those who suggest that perhaps a supposedly conservative administration that has hallmarks of secrecy in many different areas without any question, was doing something like this perhaps bore some relation to legislative prospects there. I wouldn't want to comment on that, I'm a career employee, I wouldn't want to speak for the White House or for any political

people in Congress in that respect, but there perhaps is some connection there.

So wait to see what happens with us and the one other thing I can tell you is that if you want to take a look at what we do, all you have to do is go to the Department of Justice website which is www.usdoj.gov and that gives you our main page, and if you go down to the bottom of that page you will see the letters FOIA. You click on that and you will get directly to where you want to be and you will see the extensive written guidance that we have just issued on our Executive Order implementation as well as quite frankly extensive guidance that we have issued now for approximately 25 years, including our Guide to the FOIA.

Thank you for your kind attention.

4th
International Conference of
Information Commissioners
MANCHESTER 2006

FOI : A Global Overview

Helen Darbishire, Chair FOIANet, Executive Director Access Info Europe

(Text of speech supplied)

Thank you chair.

Ladies and Gentlemen, it is my pleasure and honour to be addressing you here this afternoon.

I am particularly happy that in addition to the Information Commissioners, we have a strong representation of civil society with us today.

I want to start by reading you an extract from a short story by Nobel laureate José Saramago. The story is entitled “The Tale of the Unknown Island” and it’s a parable about how when we set out to search for one thing, we sometimes find a different, unexpected, but even better thing. At the start of the story, a man goes to the royal palace, to the door for petitions, to ask something of the King:

The Unknown Island

“The king’s house had many other doors, but this was the door for petitions. Since the king spent all his time sitting at the door for favours (favours being offered to the king, you understand), whenever he heard someone knocking at the door for petitions, he would pretend not to hear, and only when the continuous pounding of the bronze doorknocker became not just deafening but positively scandalous, disturbing the peace of the neighbourhood (people would start muttering, What kind of king is he if he won’t even answer the door), only then would he order the first secretary to go and find out what the supplicant wanted, since there seemed no way of silencing him. Then, the first secretary would call the second secretary, who would call the third secretary, who would give orders to the first assistant, who would in turn give orders to the second assistant, and so on all the way down to the cleaning woman, who, having no one lese to give orders to, would half-open the door ask through the crack, What do you want. The supplicant would state his business, that is, he would ask what he had come to ask, then he would wait by the door for his request to trace the path back, person by person, to the king. The king, occupied as usual with the favours being offered him, would take a long time to reply, and it was no small measure of his concern for the happiness and well-being of his people that he would, finally, resolve to ask the first secretary for an authoritative opinion in writing, the first secretary, needless to say, would pass on the command to the second secretary, who would pass it to the third secretary, and so on down once again to the cleaning woman, who would give a yes or a no depending on what kind of mood she was in.”

I am not sure if José Saramago is a frequent user of the Portuguese access to documents law, but this tale would no doubt strike a cord with many requestors of information around the world, used as they become to long delays, frequent silences, and eventual arbitrary and unfounded refusals of their requests.

The story also rings true for many civil society groups who know that only by knocking on the doors of state, knocking so hard and long that it becomes positively scandalous, will eventually get what they are asking for.

And maybe also the Information Commissioners see themselves reflected in the story, as they often find themselves in the role of the cleaning woman, given the dirty work of making the final decision on requests that no one else in the palace of state really wants to handle.

The global picture is positive: the right of access to information is moving forward in leaps and bounds. Not only are more and more laws being adopted (we are approaching a total of 70 laws -- which leaves only another 121 UN member states) but implementation is improving: there are monitoring studies, government reports, commissioner’s decisions and court jurisprudence to prove it.

The right to information is increasingly being respected as a right in itself, the right to know purely for the sake of knowing, and at the same time it's proving its instrumental credentials in areas such as defence of human rights and as a tool in the fight against corruption.

The two communities present here today are at the forefront of these developments: the community of Information Commissioners and the community of civil society groups working to promote and defend the right to information. This is not to exclude other actors –governments, the media, the wider public and also inter-governmental organizations– but the reality is that the actors spearheading the drive for greater government openness are represented by those of you seated in this room today.

Although having an illustrious history dating back to the 1766 Swedish Freedom of the Press act, and even back far earlier according to some historians, the right of access to information is also clearly a very young right. The fact that this meeting is just the fourth annual meeting of Commissioners, the fact that the FOI Advocates network will only reach its fourth birthday later this year, remind us of just how young it is, at least as a globally recognized human right that extends beyond a benefit granted by statute in a handful of the leading democracies.

It is a young right and it's a right that's growing up in a difficult and hostile world, at a time when the global political and security context is shifting priorities from a democratization agenda to a social control agenda. Be it well-

or ill-founded, the massive increase in surveillance of us all, accompanied by some definite increases in secrecy on the grounds of national security is impacting directly on the concept of the right to information – is it the public's right to government information or the government's right to information about the public?

The movement that promotes the right to government-held information seeks to shift the power balance in societies from the elected back to the electorate. That information can redress historical imbalances in power helps explain the tremendous enthusiasm for the new access to information laws in the transitional democracies of central and eastern Europe, as part of the recent democratic reforms in Latin America, and now in emerging democracies in other parts of the world, in Africa and in Asia.

Standards are being set right now that will define the contours of the right to information and the right to privacy for years to come. Many people in this room are involved at a day to day level in setting these standards. It is an important role in ensuring the continuity of open and democratic societies.

I am now going to focus on five challenges ahead of us if we are to strengthen and defend the right of access to information.

The first challenge is ….

1. Securing recognition of access to information as a fundamental human right.

In spite of the phenomenal progress in recent years, with national laws and jurisprudence, the right to information is not yet fully recognized at the international level, it is certainly not yet on a par with freedom of expression and media freedom. The European Court of
Human Rights has been equivocal, although it has at least recognized that information is needed to make informed decisions about how to protect family life and to maintain a clean and healthy environment.

But that may soon change: on 3 April of this year, the Inter-American Court of Human Rights held a public hearing in Buenos Aires, Argentina, in a case against the government of Chile. The case resulted from requests filed in 1998 for information about a controversial logging project, and in particular about the checks that the Chilean government ran – or should have run -- on the US-based company that planned to carry out the logging. It's not clear if the checks, such as environmental and financial probity checks, were indeed conducted, because even in the court hearing the Chilean government was less than specific as to whether or not the information existed. Failing to get an answer to their request and failing also to have a full hearing before the Chilean courts, which rejected the appeal as unfounded, the case was taken to the Inter-American Human Rights System. In the first phase of that process, successful for the applicants, the Inter-American Commission on Human Rights in July 2005 commented that there is a right to information and that the Chilean government was in violation of it. The Commission noted that:

The importance of an effective right of access to information has a solid basis in international and comparative human rights law … [and] there is a growing consensus that governments do have positive obligations to provide state-held information to their citizens …"

It now remains to be seen if the Inter-American Court of Human Rights will reinforce the existence of this right. Such a ruling, likely to be delivered by early 2007, would certainly complement the declarations of General Assembly the Organization of American States which for each of the past three years urged member states "to respect and promote respect for everyone's access to public information and to promote the adoption of any necessary legislative or other types of provisions to ensure its recognition and effective application."

Council of Europe

Standard-setting on the right to information has been largely driven by developments at the national level, while the inter-governmental bodies that limited themselves to the declarative.

That is changing however. In 2002 the Council of Europe, which represents 46 countries, adopted its Recommendation on Access to Official Documents, which, as many of you here know, lays out the essential elements of the right of access to publicly-held information and has proved useful in defending and promoting the right, including influencing some of the laws passed since 2002 in central and eastern Europe, and being a reference in legal drafting in other countries, such as helping civil society define the exemptions in the Nigerian bill.

In May 2005 the Council of Europe mandated a working group to review the possibility of converting this recommendation into a binding treaty on access to documents, a treaty which is expected to be open for ratification in 2007.

The drafting work has started and the next drafting meeting takes place at the end of next week in Strasbourg. Initial meetings of the working group indicate that the treaty will contain the main elements of the 2002 Recommendation: it is proposed that it include recognition of the right of access to official documents, and consideration is being given to the broader formulation of a right of access to information, to take full account of the range of European norms. It is proposed that the list of exemptions set by the treaty be a

definitive list: signatory governments would not be permitted to add other grounds for exemptions – and be subject of course to harm and public interest tests.

The definition of bodies to be covered by the obligation to provide information will be broad, including all bodies performing public functions. The specialists working on the treaty are mostly experts in the field and committed to openness. Civil society is being consulted. All is well.

The biggest obstacle is likely to be not the content of the treaty but the monitoring mechanism. Unless there is a strong monitoring mechanism, a treaty be not differ significantly from the current Recommendation.

Some European governments have expressed reluctance to commit to a full monitoring mechanism, and it has even been proposed that the monitoring body meet just once every five years. This would be a real problem and would take the teeth out of the treaty.

The problem, it is argued, is that a regular monitoring mechanism with capacity to review periodic reports form signatory states and conduct study visits would be too costly. Interestingly, other monitoring mechanisms do receive funds, such the GRECO process that monitors compliance by Council of Europe member states with anti-corruption principles.

The real problem, put quite simply, is that access to information is not yet seen as being a political priority in the same way that defense of other human rights or the fight against corruption is. This is a challenge for all of us, particularly in the Council of Europe region but also more widely as this treaty will create a model for international supervision of the right and could become a strong complement to the work carried out nationally by Information Commissioners.

I would urge those of you whose governments are in a position to influence the decision on how the Council of Europe treaty on access to information will be monitored, to encourage your governments to make this treaty a priority and to commit resources to the monitoring mechanism.

Italy and Dominican Republic

A further element in defining the right of access to information is not to tolerate sub-standard laws and violations of the right at the national level, particularly in countries purporting to respect the right.

There are a handful of countries where the right to information is enshrined in law but at the same time the law restricts the right in its very essence. One such country is the Dominican Republic where an otherwise excellent law requires requestors to state the reasons for their requests.

Another such country is Italy, where the relevant sections of the administrative code establish the right to request administrative documents but require that

the requestor to justify the reasons for requesting the information – essentially that the requestor has to demonstrate that the information is needed to protect a legal interest or because the requestor is in some way party to an ongoing administrative process.

Such requirements are unacceptable and will breach the future Council of Europe treaty. In the meantime, the community of nations involved in standard-setting needs to ensure that legal regimes containing such flagrant breaches of the right are not counted when listing countries that respect the right of access to information, and such breaches should be condemned wherever possible.

2. Defining exemptions – and what information should actually be made public?

The second challenge facing us is the need to define yet more precisely the exemptions to the right, and to define also, and more specifically, what information should be entering the public domain, either proactively or through requests for information.

There is increasingly a commonly agreed if not perfectly aligned set of exemptions to the right to know. The challenge is to ensure common interpretation of those exemptions, because in practice the picture is rather messy.

Take the issue of the application of the commercial interests exemption to access to government contracts with private suppliers. In more developed information regimes, copies of contracts and/or the majority of the information in them is available. There is good jurisprudence from the courts, in older FOI regimes such as the United States but also in newer regimes such as Israel, where several court verdicts about access to government contracts have firmly established that when a commercial entity makes a contract with government, the commercial entity is accepting to put itself under public scrutiny.

In addition to the courts, there are the Information Commissioners, who have issued strong decisions, such as that from the Irish Commissioner ordering the Department of Finance to release details of contracts with advisors, in one case noting that a contract payment of some €850,000 is a “large amount of public money.”

The Slovenian Information Commissioner similarly has ruled that a contract between a local municipality and a housing management company (run as it happened by the deputy mayor), should be released. The decision elaborated an excellent set of criteria for assessing what could and could not be classed as a trade secret. The Commissioner even suggested that if bidders for government contracts declare large parts of the information they submit to be trade secrets, the contracting agency should exclude the bids.

But in spite of this, even in countries with reasonably well-functioning access to information laws, it's still extremely hard to get copies of a government contracts. In Bulgaria, the Access to Information Programme, an NGO with a a good record of winning litigation and securing information, last year lost a case at the Bulgarian Supreme Administrative Court for access to the contract between software supplier Microsoft and the Bulgarian government. The contract in question relates to a deal with a value of $13.5 million – definitely a large amount of public money by any consideration.

Similarly in two cases which are still awaiting court decisions, the Albanian government is refusing to release details of the contract for the privatization of the state telecommunications company and the government of Montenegro recently declared that the entire part of all privatization contracts are business secrets. [The government of Montenegro can be congratulated on achieving independence on Sunday, and now we can add another national FOI law to our lists, but it's transparency policy clearly needs some more work.]

The same patchy picture can be found with access to other classes of documents. Assets declarations for example can be downloaded from the web in Romania, but you need to be a journalist to access them in Bulgaria. In Argentina the are available under some regional laws, but in Peru when the assets declarations of government ministers were requested, the ministers got together in a Committee of Ministers meeting and decided to give out only the summary sheet rather than the details. That's not good enough because for

anti-corruption monitoring it's precisely the details that are needed to spot changes in assets held and so to identify possible illicit enrichment.

When a regional government in the north of Peru went against this decision and published the assets declarations of all local councillors and officials, they received a letter from the State Audit Office warning against "excessive transparency", although failing of course to point to any specific harm that was being done by this over-enthusiasm for openness.

The criticism of being overly transparent is not one that public officials will take lightly in countries with a traditional culture of bureaucratic secrecy. We know from experience that strong comparative arguments about what information should be released can be of tremendous help in convincing public bodies that they are not at the cutting edge of transparency standards in releasing certain information, that they are operating within a safe zone. To achieve this, there is room for more research into and dissemination of comparative standards.

3. Defining the bodies covered by the right to information.

Challenge number three is about defining the bodies that are obliged to provide information. Here in the UK the law is very broad in scope and obliges a vast range of public bodies, basically covering both the public functions principle and the follow-the-public-money logic of comparative standards. 115,000 bodies is indeed an impressive number -- as I know from the reactions I've seen when I have mentioned it to law-makers around the world.

As the right to information develops, issues arise about the appropriate reach of the right to request and receive information. Last year, Argentina failed to adopt a draft law because of protests over attempts to oblige private bodies to release information. The proposed amendment read that “private bodies, both for-profit and non-profit, that have a public aim or hold public information”. What this definition would have meant in practice is not clear. Civil society and media feared potential abuse, for example by forcing journalists to reveal confidential sources of information or NGOs to answer requests for sensitive human rights research materials.

Certainly the proposed provisions in Argentina were overly broad by current international standards. The questions is what are the appropriate obligations to place on private entities. The most progressive laws, such as the South African Promotion of Access to Information Act (2000), do place obligations on private bodies to respond to requests for information, but only insofar as the information is that “required for the exercise or protection of any rights”.

If it’s the right information is to serve to equalize power balances within society, then some attention has to be given to private companies. With many multinationals having annual turnovers and capital assets in excess of most small countries, the power they wield is phenomenal. The public needs information about the practices of private companies that impact upon matters of human rights and quality of life.

The question is, where should the public to go to request that information, to the private companies or to government oversight bodies and regulators? If it is to be the latter, as the current right to information paradigm suggests, then these government regulatory bodies need to be obliged to gather information.

In the US there is currently a battle going on to stop the Environmental Protection Agency from changing the criteria for reports that companies have to make according to the Toxins Release Index as well as the frequency of that reporting. The concern among environmentalists and others is that these changes would reduce the amount of information that the EPA holds, and therefore reduce public access to this information, even though the private companies would still have the obligation to gather and hold this data. There is currently a bill in the US Congress to block the EPA proposals.

Increasingly, FOI activists and Information Commissioners are being called upon to pay attention to issues of data-gathering and information creation. This opens up a whole new area where comparative norms need to be developed on the types of information that government bodies are obliged to hold if the right to information is to be fully enjoyed.

There also needs to be some serious debate about strengthening obligations on private companies to release information directly to requestors.

4. Supra-National Transparency

Challenge number four relates to supra-national transparency. With all the progress that is being made at the national level, supra-national bodies are now falling behind with respect for the right to information, even if those same inter-governmental bodies are engaged in the process of promoting national access to information laws.

A group of NGOs called the Global Transparency Initiative has been working with supranational bodies such as the World Bank and other development banks, and has had some positive impacts: the Asian Development Bank for instance last year made the paradigm shift from a disclosure policy based on a presumption of secrecy to presumption of openness with limited exemptions.

There remains the problem of securing access to documents held by international bodies when it is not clear who “owns” the documents.

Even though most national laws oblige public bodies to release information that they hold irrespective of which body was the originator of the information, at the national level requestors sometimes come across the problem of a government refusing to release information related to its relationships with supra-national bodies on the ground that the international body was the originator of the document and is therefore the owner of it.

There is some useful jurisprudence on this: in Georgia a court ruled that once a contract had been signed with the World Bank, the funds became part of the

Georgian state budget and related information was subject to the access to information law. Similarly, in Costa Rica the Constitutional Chamber of the Supreme Court has ordered the release by the Central Bank of International Monetary Fund reports about Costa Rica's economy.

The European Commission, in a Green Paper published on the 3rd of May of this year about the transparency of EU funds states that whilst the EU "as a driver of change and modernity" would like to be releasing more information, in spite of the "additional administrative burden" that this entails, it is often put in a difficult position because if a member state is not ready to disclose the information, the Commission cannot, because it does not have the right to hand it out without the prior agreement of the Member State concerned.

The Commission notes that only 11 out of 25 member states are making public information on the Common Agricultural Policy and even then with wide variations in the degree of detail available and the procedures for providing access (ranging from total and direct access to partial access on request). Similar problems of access relate to data on Structural Funds, and to the beneficiaries of the Financial Instrument for Fisheries, which are placed on-line in just 5 member states.

The amounts of money being talked about here are really huge: around 75% of the entire EU budget, or about €87 billion per year, all EU taxpayer's money. There is compelling evidence that in a number of countries the lack of transparency is facilitating corruption and diversion of funds.

Interestingly, the European Commission, in the Green Paper, notes that : “the restrictive approach taken to publicity by some Member States is often based on national law or practices on data protection, which vary from one country to another beyond the minimum requirements set at EU level and are often determined by different national traditions and cultural perceptions and sensitivities.”

This is a controversial claim and I am not at all sure that data protection is the full story. But whatever the reasons, the information is falling between the cracks, between the national governments and the supra-national organization, and the public cannot access it. The EU should be encouraged to ensure that it is able to release information and at the same time any problems at the national level should be addressed, to ensure that the buck cannot be passed back and forth between the national administrations and the international body.

The European Union is an important case study because of all the international bodies it comes closest in nature to a government and therefore the standards for transparency that are set at the EU will provide models for other similar bodies around the world in the future.

UN Requests

Finally on the issue of access to information related to international bodies, last week requests were filed in about 20 countries for information about how

the world's governments voted in the election of the UN Human Rights Council on 9 May. The vote was secret and it is therefore impossible to know whether our governments voted for countries with poor human rights records. This initiative started when the Chilean senate (I think that I mentioned before there are some activist senators in Chile) asked the Chilean government how it had voted and it refused. So, in the coordinated filing of requests, made around the world, including by a number of people here today, we asked to know both the vote and also the criteria used to assess the human rights record of the countries voted for. Some of these requests may eventually come across the desks of the Information Commissioners here as it is likely that the international relations exemption will be applied. As with all the other exemptions, there are of course instances in which protection of international relations requires secrecy, particularly for the limited period of time while negotiations are ongoing. On the other hand, when decisions have been taken, particularly decisions which affect human rights, the public interest should prevail. One of the ways in which we are going to open up the supra-national institutions will be through release of information at the national level, and this is clearly another area where sharing of information, decisions and jurisprudence is helpful in setting the appropriate limits to exemptions and ensuring maximum access to information.

5. Commissioners

The fifth and final challenge relates to the role of Information Commissioners.

I don't need to tell you gathered here of the value of Information Commissioners in ensuring the successful implementation of access to information laws and in drawing the appropriate limits around the interests that need protecting, be they national security, privacy or commercial interests. But I think that there are a lot of people we do need to tell about it: there are still too few access to information laws that establish these institutions.

There are some models of Information Commissioners that are increasingly well known: the Mexican IFAI, hosts of last years Commissioner's Conference, and this year's hosts the UK Information Commissioner's office. The problem with these larger institutions is that they are often seen as too expensive and governments are reluctant to commit. It's not "resource neutral" to use a phrase we heard this morning.

That's the case right now in Chile for example where the constitution has been changed to include a right of access to government documents and the new government of Michelle Bachelet has committed to adopting a law, but has expressed doubts about a commission. In part because they are aware of the Mexican model and see it as a large and expensive undertaking.

It would be going to far to claim that without an effective independent oversight body, the right to information is not respected. As long as there is recourse to the courts, there is protection of the right. But that's to overlook the wider role that Information Commissioners play: providing guidance on institutional reform, training of public officials, educating the general public and developing systems like the SiSi request submission portal in Mexico, monitoring compliance by government bodies and taking action to address problem areas … there is much that Information Commissioners can do, and somebody need to be doing this work for the right to information to function effectively. We often see that in countries without Information Commissioners, civil society has to step into fulfil the role of public awareness raising and even training of public servants. The nature of the right is such that it requires action and oversight. No government would think of running elections without an electoral commission. Data Protection Commissioners are recognized as part and parcel of protecting the right to privacy; the same needs to be achieved with Information Commissioners.

This means overcoming arguments about costs and demonstrating the utility of Information Commissioners. Avoiding the costs of lawyers and the burden on the court system is part of it, more efficient information management and better-informed decision making is another part of it. These are not always visible savings and may be hard to quantify, but neither should they be overlooked.

A greater variety of models needs to be presented to countries considering commissioners, to Chile and also to Uruguay, Croatia and Moldova. In Uruguay members of parliament are interested in the Slovenian Information Commissioner model: it's on a more appropriate scale for the small country than the Mexican model, Slovenia's population is a similar size and its macro-economic indicators and democratic profile are ones to which Uruguay aspires. I propose that we discuss how the FOI activist community and Commissioners can share their experiences with countries where laws are in the process of being drafted or reformed. For example, Chile looks to New Zealand and Ireland as models and would be interested in the oversight functions there. Even a simple study trip costs money of course but, the readiness of the Commissioners to host such visits would facilitate such trips and even could help with securing funds.

HOW TO ADDRESS THE CHALLENGES

So those are some of the challenges in front of us. To finish I'd like to look briefly at how they can be addressed. Three ideas:

Number one is Money, of course: more funds are needed to ensure continuity of the work of civil society and the work of Information Commissioners. Money is needed for the international human rights bodies to monitor the right to information, and for the monitoring mechanism of the future Council of Europe treaty.

This means that the donors – both governmental and private donors -- need to be convinced of the utility of protecting the right to information and they need to understand what nature of the work that needs supporting. Civil society groups know only too well that funds are more easily available for campaigns to adopt access to information laws than for the laborious technical assistance work of assisting with implementation, conducting monitoring and undertaking litigation.

Support is also needed for sharing of best practices between the Information Commissioners. The World Bank for example is providing support to the IFAI for wider distribution of the SiSi request filing system. There is much to share if resources are available to help us share it.

Number two: Information sharing – Even with limited funds, I believe we can further improve sharing of the body of knowledge being built by civil society and Information Commissioners. The FOI Advocates Network has around 70 member organizations and a mailing list of about 200 individuals. The main discussion list contains dynamic exchanges. Anyone on the list can request information on comparative law and practice on a wide range of access to information issues, and answers are usually received within hours of the requests being posted on the list. Some of the examples I have given in this presentation are taken from recent exchanges on the FOIA network. A few commissioners are on that list, but we could if any more would like to join, you would be very welcome. Let me know if you are interested.

Number three, Right to Know Day – my last point is to note that NGOs working on freedom of information have nominated 28th September as International Right to Know day and the idea has been picked up around the world; last year there were events and media activities to mark the day in at least 30 countries, and although not yet a formal UN day, it has received some recognition from intergovernmental bodies such as UNDP.

I believe that much more advantage can be taken of International Right to Know day to promote the values which all of us here share. Having an annual day provides a platform for reaching out to the public and raising awareness of the right to request information from government, the right to know what the government knows, the right to know how taxpayers money is being spent and how power is being exercised.

It would be wonderful if the Information Commissioners, either as a body or individually would also mark Right to Know Day and so help to maximize its potential for raising awareness of the right to information.

At the end of the short story by Jose Saramago, the man gets to see the king, who gives him what he is asking for, which is a boat, and he falls in love, with the cleaning woman in fact, and together they set out to sea in search of unknown islands and other new discoveries. I wish you all such happy endings.

4th
International Conference of
Information Commissioners
MANCHESTER 2006

FOI Regimes and Other Statutes – interfaces, conflicts and contradictions

Part 1. Tony Bunyan, Director, Statewatch and European Civil Liberties Network.

Part 2. Peter Hustinx, European Data Protection Supervisor

Tony Bunyan

I'm going to talk about Freedom of Information, and I'm going to talk about Data Protection, but I'm going to start out talking about the context because Data Protection and Freedom of Information do not exist in a vacuum and therefore given what we do in looking at civil liberties in the European Union I'm going to start out with that general context of our work in these two specific fields.

I think there is a lot of misunderstanding about the difference between attitudes in Europe to the war on the axis of evil- Iraq, Iran, Syria etc- and the war on terrorism, which is quite different. So while there are major differences over the war against the axis of evil there is little or no difference between the EU and the US on the war against terrorism. There is a difference of timing, a

different emphasis, a difference of language, but there are very few differences. Indeed an axis has grown up, what we call the EU/US Axis, so that the USA is now sitting in on Council working parties, holding meetings with the Presidency, and indeed if one looks at the influence of the United States on EU policy they have almost become the 26th member of the European Union.

So when we look at that ideology on the War on Terrorism, I would distinguish it. I think it's very important to understand the difference between the War on Terrorism and the previous era of the Cold War. The Cold War was a time when because of nuclear warfare possibility our way of life and our democracies were under genuine threat of being destroyed – genuine threat, I lived through that era. But the current War on Terrorism, terrible though it is, with the terrible deaths that have occurred, is *not* going to destroy our democracy or our way of life. What *is* going to destroy our democracies is the reaction of our governments to that terrorism. I think there is a sort of gulf of understanding. What we find in a civil society is that we are looking at the same world as the EU government and officials are, but we are coming to utterly different conclusions about what the problems are and what the solutions are.

There is an idea in the European Union that somehow we have shared values so the idea is that all the measures they have taken since the 11th September 2001 have properly balanced security and civil liberties. That is their attitude. Or what Mr Solano has said – "Our way of life hasn't changed". To the first

point I would say, if what has happened since 11th September in our field – Justice/Home Affairs – and I am meant to share those values, I do *not* share those values, nor do millions of other people. We fundamentally disagree with the direction that the EU is going in. But our way of life hasn't changed they say. Mr Solano said it, Tony Blair has said it, Mr Grittini has said it, the man in charge of the Commission. But whose way of life? The white western European way of life? Because certainly the way of life for my group of communities, the refugees and asylum seekers, has changed enormously since 11th September, so have attitudes towards them.

I'm reminded of two very quick examples. One example was a picture we published a couple of years ago and it was in Spain, a person was sunbathing on a beach and 50 yards away from them on that same beach, was a dead refugee. In another picture we published, there were people playing beach ball while two dead refugees were being removed from the beach in their full sight. And this told us something about not just Spanish attitudes but attitudes towards the plight of migrants.

I'll give you one example which does relate to access to documents. For many years now the EU has been sending people back to the countries they have come from or the countries they think they have come from. Now they are increasingly organising joint flights, bringing a few people on one plane back to Africa. Tens of thousands each year are sent back, often through the IOM, the International Organisation of Migration. But I will tell you something. The European Union, when it comes to cattle, cattle, because of money, it

knows where every cow is, and knows the condition it is being kept in. But I will tell you something else. There is not a single report in the European Union telling us where the people are who have been sent back, repatriated, or what condition they are living in – not a single report in the whole European Union. And if those are values I am meant to share, I do not.

So there are connections here. When we looked at what happened after the 11th March, the dreadful bombings on the train in Madrid, and we looked at 57 measures, and you may have seen on the website we made a scoreboard and went through each of those and judged them according to their relevance to terrorism, and we judged that only 27 out of 57 measures had something to do with terrorism. The rest had little of nothing to do with terrorism. It's been referred to before but it's become a continuum now that when you talk about terrorism, you talk about organised crime, about money laundering, serious issues, then you talk about *all* crimes. In other words, the word terrorism has come to contaminate everyday law enforcement in the European Union.

There was one report they published, a proposal which said, "But we've got to monitor all mobile phone calls, because terrorists use mobile phones". Does that mean that *everybody* who uses a mobile phone is a potential terrorist, which is the implication? There is a dreadful logic going on that if you justify it as an act of terrorism you can do anything. And I think this is the danger we are facing at the moment. What we know is that there is a whole series of measures currently being discussed in the European Union. Now these include, not just the exchange of passenger name records with the United

States, they include the EU's own passenger name system, of everyone flying in and out of the European Union, not just people with visas but everybody flying in and out, with the historical record. It includes, which went through just before Christmas, mandatory retention of telecommunications data, biometric visas, biometric country national residence permits, biometric passports, discussion of the biometric driving licences and in time health cards with your personal medical record on it. We are heading for the situation where we will have one card in the end which tells the whole of our life, I think most of you know this, but I do not think most people in the European Union realise that when they want to renew their passport in what, a year's time, they are going to have to compulsorily present themselves at an enrolment centre, be interviewed for quarter of an hour to prove who they are, to compulsorily have their finger prints taken and in some countries to have a facial scan taken as well. I do not believe the people in the European Union know that is going to happen. We know probably because we are looking at it, but I don't believe that is widely known.

And there is this dreadful thing about the continuum to the point that if you *do* want to tackle terrorism, and I have no problems with trying to tackle terrorism, you have to understand who is going to stop terrorism. Or as somebody put it, what you need is intelligence, intelligence, intelligence. That's how you tackle terrorism. That's the Security and Intelligence Agency's job. The role of the law enforcement agencies is secondary. Anybody would tell you that if you know anyone in the security world. Human intelligence is the most important and this takes years to put in place, to train people, to go

inside and find out what is really going on. That is how you stop terrorism. You do not stop terrorism by putting everybody in the European Union, making everybody a subject and putting everyone under surveillance in the minutiae of everyday life.

That's the broad background. Now within that we have fought over the years on access to documents, and I'll briefly go through some of the problems we have still got in the European Union over access to documents. Over the regulation that was part of Regulation 1049 2001, there are some problems with the European Parliament that they don't publish a proper annual report, there are some problems with the Commission as they don't have a proper register which they are meant to have. The biggest problem of course is, as is almost inevitably, with the Council. The Council is by far the most powerful body in the European Union, that is the body of the Government.

What are the problems? Well one of the biggest problems starts right at the beginning. It's when those 25 Prime Ministers meet at Summit Meetings. Now we have a thing called the Hague Programme which includes the principle of availability of all data to all law enforcement Agencies across the whole of the European Union and almost anywhere in the world. That was adopted on 5th November 2004, but was the Hague Programme discussed by any national Parliaments before it was adopted, by the European Parliament? Was it published so that civil society could look at it, take part in the debate, make its views known? No. It was drawn up by government officials and adopted literally on the nod because they had other business at the time, and that set

the Agenda for the whole of the European Union. It set the Agenda for the Council and therefore for the Parliament and for the working parties. This is the most undemocratic way to run anything.

This is the problem with the European Union – it is one of the most undemocratic bodies I have ever known. You look right back through history Hundreds of measures, all of which had to be adopted by the enlarged countries, countries that joined in with the Enlargement, none of those were subject to co-decision in the European Parliament, none of those went through national parliaments. It is a democracy built on sand in that sense.

Now we have exceptions. We have the famous 'space to think'. So we get refused documents because we're not allowed to have it under discussion. I'll explain to you why that is terribly important. In a democracy, it's terribly important that the parliament and civil society, the people, know what is going to be 'on the table', know what has been decided and know what discussions went on that went to framing that particular measure, before it is adopted. What they are saying is that if you cannot have access to documents until we have actually adopted the measure. Now you don't do that in a democracy. In a democracy you make it clear to people – this is what's on the table, these are the debates, these are the issues, parliaments and civil society can debate it, have their influence and at the end of the day you can accept their decision. What they're saying is that you cannot have access to these documents until the measure has been decided. Is that democratic?

And then we have a problem with third parties, particularly with the United States, where we are routinely refused access to any document or almost any document, where there has been a meeting with the EU and the USA. I won't dwell on this but one more point to make is that we do have in the Regulations the idea, which a great fuss was made over, the idea of 'public interest', in other words, we could claim, if they refuse the document, that it was in the public interest, that if they intend to monitor all the telephone calls of everybody in Europe, have access to all their emails, it might just be in the public interest that we should know what's in that proposal, or an aspect of it.

Do you know, there is not a single appeal, based on public interest, which has ever got through in the Council or the Commission. The concept of public interest as a way of getting access in the European Union is absolute nonsense and doesn't work. They take the view that it is in the public interest that it's kept secret, in 100% of cases. This is a nonsense.

I'll now move on to some of the linkages in a sense between Freedom of Information and access to documents and Data Protection. I think I'll start out with this lovely principle of availability. We have to talk about this – can you have Data Protection and the principle of availability, can they co-exist? The answer is, of course not! But we have got it, because the Hague Programme says we've got to have it. Where did the idea come from? How did it get into the Hague Programme? It got in the Hague Programme in 2004 because it had already been discussed in G8. It went from G8 into the EU Presidency and then into the Hague Programme. That's where it came from – we can

track it, we can document it. And when you look at some of these document which are coming in and I have brought along three examples, the first of which is the meeting on 11th May 2006 which we're not meant to have of course, the outcome of the EU/US ministerial troika on 3rd May 2006, and in this it says, quote point 6," is concerned that some of the new rules, for instance Article 15 on the transfer of data to third parties, this is in the measure we've got on third pillar of Data Protection, might weaken the current co-operation on the existing agreements".

In other words, the United States is opposed to what is in Article 15. This is about the third reference I have seen to this in different documents. We are not meant to know the United States doesn't like Article 15, about the transfer of data to third parties, because the document is secret. We also know from other documents that the US is making demands for access to the SIS, to SIS Two, to the visa information system, when we have got a fingerprint database it also wants access to that. We know that, but we're not meant to know that because all of that is in documents which are not public. I think we have a right to know what is in those documents.

Now in the same document, this same document in Vienna, it says, and this is going to be quite interesting, this is about visas for the United States or actually EU passports to the United States, "The US expressed satisfaction with the progress reached so far, and invited the EU to assess how access for verification into E-passport databases will be organised". In other words, the United States is demanding access to EU or national databases for

anybody who goes to the United States. Is that going to happen? Is it going to happen without a debate? I don't know.

I want to move to a big issue now. This is the whole idea of passing data to third states. When they first got these agreements that Europol could pass data to third states, at the beginning I remember we looked at it, and one of the states we looked at was Norway. We looked at the assessment of the Norwegian law. We sent the EU report to our friend Thomas M……. in Oslo and asked him what he thought about the assessment. He said it was a good theoretical statement of the state of the law, but there was nothing in it about how the law actually works in practice. All those assessments about the exchange of data in Europol and third states are based on the theoretical, constitutional, legalistic position in the law. None of them contain detailed case law problems, controversies, scandals or anything else. It is sheer nonsense.

But now let us look at a real beauty. This is this famous Europol/USA Co-operation Agreement which had to be passed on 6th December 2001, and added to on the 20th December 2002, because of the War on Terrorism. Now I have got here a report which is very intriguing because this report is quite old. This is dated 27th July 2005. It is 10 months old. It's still secret. It is the mutual evaluation of the Co-operation Agreement of Europol and the United States. And what does this document tell us? It is only a limited document, not a classified document, secret document in that sense, but it *is* secret because it is not available. So what do we find? We find that on the US side,

apparently, which doesn't surprise us of course, "Competencies are assigned to a variety of Agencies - Federal, State and local level" . But actual exchange of data which is meant to all go through Europol, doesn't all go through Europol. Some of it goes through Europol, a lot of it though goes through the seven member state of seconded officers and offices in the United States – Belgium, France, Germany, Italy, Spain, Netherlands and the United Kingdom. A lot of it also goes through the Attache the United States has in the European Union. So only a tiny percentage of exchanges are actually happening through this terribly important, terribly necessary Europol Agreement. What we then discover, they say that Europol is generally not approached for making requests to member states by the USA because they use long-established bi-lateral channels. And then most damning of all it says of course, even though it's meant to be a mutual assessment, is no centralised statistics are collected by the USA on the exchange and transactions with EU member states. In other words, they don't know, it would appear they don't care, there are no figures whatsoever. So how can it be claimed that the Data Protection provisions, allegedly in that Agreement, and of course there are other agreements yet to be implemented, the agreements on exhibition, the agreements on mutual assistance, because we all know that the United States has got so many Agencies they've got no idea whether this information has been passed on or who it is being used by, and this is the first fault we have which is confirming that this is actually happening.

The third document I've got is one relating to the principle of availability. This is quite interesting because the document *is* available on the register. It's a nine-page document, except that the version on the public register is only partially accessible. So only the first four pages are accessible, five pages are therefore not accessible. However, I have a copy of the full document, so what is it that they are trying to suppress on this occasion? Well it's the fact that they are actually using the Pro…..Treaty as a point of reference. The Treaty, and this is funny the European Union if you don't come from here, a little group of countries, Germany, France, Spain and others, decided to set themselves up as their own little council, adopt their own little treaty, which has no locus inside the European Union, but you have got a major Council working party here determining policy according to this Treaty, which hasn't been adopted or agreed yet, let alone having no locus in the European Union! But what are they discussing and what are they hiding? Well of course it's DNA, fingerprints, vehicle registration databases. It's very interesting what it says. Regarding DNA databases, "This would obviously imply that all member states establish DNA databases for the investigation of criminal offences". Note it says "criminal offences", it doesn't say serious criminal offences, *any* criminal offence. And it also says that member states "have to establish automated finger print identification systems if they don't have them already".

DNA is quite interesting actually because, what are the figures? Austria 0.98% of the population, Switzerland 0.83% of the population, Germany 0.4% of the population, United Kindgom 5.24 %, but they are titchy, and of course

the United Kingdom is very interesting, because we weren't meant to be keeping all these DNA prints. Even if suspects are not charged, their DNA can be held forever. So you can be arrested as a suspect, questioned but not charged and your DNA can be kept for the rest of your life, or you can be put on trial and acquitted and still your DNA can be kept. Now obviously these other countries in the European Union are not doing this. The UK in this instance is leading the way in terms of what DNA is going to mean.

It is quite interesting and it has been noted by others, that in the first… reached by the Commission, which is Data Protection on Policing, and Judicial Corporation, which of course leaves immigration and asylum under the existing law 1995, but it has got a little footnote there which is now in the latest version, it's got LS Version which means the Legal Service of the Commission, it says "Nothing in this must restrict or prohibit the principle of availability". In other words nothing that goes into the Directive, must prohibit the principle of availability. That's been repeated. That's in the official version now. And when I read things like special categories that you should not keep information of racialistic critical opinions or of ethnic origin well I'm a bit cynical about that because the UK for example has always derogated from that provision of the Council of Europe Convention.

This is though the one that really worries me. "Things are authorised, providing they are lawful", providing the law says Parliament's passed it, it's in the law therefore it is valid to exchange information. But what if the laws being passed are themselves bad laws? What if they are authoritarian?

What does this mean – Glorification? What does it mean if you are arrested and your DNA is taken, but you are never charged? What does it mean if you have got an anti social behaviour order, some of which are valid but many of which are very silly? What does it mean if you are under a control order, which people are under now? This is the problem. What is becoming lawful now, would not have been lawful 10 or 15 years ago, we wouldn't think of passing it.

One of the problems we have got is that many of the laws that have been passed at European Union level, the measures being agreed, when we reflect, as a body of law, biometric passports, DNA, passenger name record, data retention, they are all measures they would have never have dared put through during the Cold War. Because they are all measures of the kind they accuse the Soviet Union of abusing Human Rights on. And now we're doing it, now it is happening. I think we are living in very dangerous times.

Access to documents is a means to an end. It's very important to fight for but once you've got the document you have then got to be able to use that document, explain the relevance to people, explain the dangers in it to people. So access to documents is a means to an end.

Data Protection is also only part of the picture. Data Protection *isn't* civil liberties. It is an aspect of civil liberties. The other aspect of civil liberties isn't just the data that is transferred, it is how you are treated. What happens when you are arrested in the street, in your home, how you are treated at the

police station, are you allowed a lawyer quickly, are you allowed a translator? That's the force of liberties, which data protection is just a part. We need a broad democratic agenda which does include Freedom of Information, does include access to documents. What we also need is not another fundamental human rights agency for the European Union, what we need to see, and this is quite extraordinary, the European Union fundamentally believes in the European Convention on Human Rights – we are all signed up to it. How many of the 25 member states of the European Union have got Human Rights Commissions? Five, out of 25. Why don't we have a Human Rights Commission in every member state by a Directive, according to the Paris Principles, which means they have got to be independent of government and properly funded? There are bigger questions to ask so what I am saying is that that the issues we have to be concerned with are part of a broader democratic agenda and if we are going to resist this shift which is getting faster towards authoritarianism, it needs you in this room and civil society at large, and our allies in parliament, to work together to try and see if we can reverse where we seem to be going now.

Thank you.

Peter Hustinx

My intention is to briefly discuss some of the interfaces which seem to be relevant to FOI and then move in the second half of my presentation to a report I published in the middle of last year on the interface between public access and data protection, and frame this with some references to relevant case law.

In terms of the overall legal framework I work against and in, I want you to know without going into details that in all these treaties and in fact also within the constitutional treaty which has not been ratified yet, there are a number of very clear references to openness, to transparency, to respect for fundamental rights, to privacy and data protection especially and there are provisions of explaining how the balance should be struck but in a very general fashion. What is interesting also is that in the Constitutional Treaty which integrates the EU Charter, not a binding document either but a document with some authority adopted in 2000, data protection and transparency – public access – are put together. You see this in chapter1-50 and 51 in a section dealing with the democratic life of the Union. Both are seen as principles of good government and they are discussed together.

If I tried to be bold and present a very brief analysis of an FOI claim, it is perhaps fair to say that depending on the legal system you work in, it may have been formulated as a right, that is probably the nicest way to do it, or an obligation to provide information on request or spontaneously, the scope of these laws could be general or specific. Then there is an obligation or right to

be provided with access to existing information sometimes it is framed in terms of documents, you know the differences, and documents are likely to have a very general definition, is a claim which could be made by any member of the public and that is a very meaningful point to which I will come back. But no special interests are required to make a claim under FOI. Many of these laws provide for information delivery on request and they encourage direct provision (this morning it was referred to as affirmative or proactive publication) subject to all kinds of limitations.

I see three types of limitations: what was referred to this morning as the "Freedom to think", internal considerations that is time bound, it changes quality as the decisions have been made and then there are different kinds of public and private interests which you can imagine I don't have to repeat here.

If we look at some of these interesting aspects and think around this claim, then there is first of all the question of the scope of the FOI Law. In the case of the European Union, it is a regulation, which applies to three institutions. This is because the Treaty simply refers to these three institutions, but there is a general practice to apply this to adopt this via internal rules and other mechanisms to all other institutions and bodies. That is a model which may be of interest to you or it may in fact refer to your own situation. Now if that is not the case, then you may have to deal with a number of statutes and then the question of which statute, which claim has priority, the problem of the specialist and generalist. On a European level as on a national level, a famous example is the environmental transparency in the Aarhus Convention

and many directives translate this into national obligations, but there are many examples of special registers which provide specific transparency on civil status on real estate and other things you will no doubt recognise.

An interesting question it seems to me is whether the FOI law is perceived as an open system or as a closed system. If it is a right to be provided to information, subject to certain limitations, what if the right doesn't apply, does it mean that the limitation basically acts as a secrecy system or is there room for other legal basis to come in? And one of the possible legal basis not often seen this way but in my practice I come across it quite often, is that data protection legislation provides the basis for various ways of transferring data to specific third parties and it may well be that the good execution of a public task provides for specific transparency under specific circumstances, quite apart from the FOI Regime.

If we think about beneficiaries of FOI, then any member of the public does have some consequences as it means that no reasons are required, you don't have to say why you are interested, there are not conditions attached to making a claim so it's not a special interest, and the question is also is it acceptable to provide information, to make it available , under FOI, with conditions attached, if there is an acceptable mechanism to privilege certain members of the public and say OK you can you have this, subject to conditions. In my view this is not acceptable.

But what about specific interests? There are quite a few and I will mention some examples: The Data subject under Data Protection law has a very special right of access to his own personal data. In exercising his right, he could come across data which also relates to a third party – so there you have a third party conflict as well. In European law in the staff regulations, there are a number of specific employees' rights. Access to a personnel file is covered by Data Protection law as well, but there is an obligation to publish certain decisions by employers so as to enable the employees to challenge these decisions, non promotion of promotion and things like that. There are a number of special rights which are specific in relation to FOI. Sometimes this distinction is not clearly made. This morning when Richard was referring to the DTI investigation, I was wondering on what grounds the FOI claim of the company having a special interest were entertained.

Now committees or members of parliament, parliaments have special rights under constitutional law but they usually take a majority unless the minority rights are protected. If the decision of the parliament has not been taken, what is the situation of the committee of MEPs. I will come back to a famous example in the European Union where a member of parliament was in his role as a member of parliament using FOI to remake the constitutional debate in parliament work better. And that always questions in international administration corporation or between departments, governments. Sometimes these requests are FOI, sometimes they are not, time does not allow me to go deeply into this.

Then if we look at exceptions, obviously there are different kinds of exceptions and laws around the world will be different, but in my practice a basic distinction is between the absolute and the relative exceptions. That is, the absolute applies and they have consequences and all the debate is then whether the exception applies. What is exactly the scope? In a relative exception, all the effort is in the balancing of the interests and there are intricate systems to do that.

And the position of confidentiality, in the early days principles of confidentiality were held against FOI. Of course that does not work . That does not mean that confidentiality doesn't have any role. It seems to me that leads to a default position if there is not an obligation to share information then there is a general rule of prudence, secrecy is a special case.

Sensitive documents in different forms such as state secrets are specially restricted, in many schemes have a special place, and there you have the interesting phenomenon that the code which is put on a document at a certain date has to have its effect when the FOI claim is made and then the question arises who is really on what under the present circumstances of the case is the legitimate answer.

Here I have a fourth interface – it is a fascinating one as far as I am concerned – think about the position of archives. Just move the clock and see what the time does then you will see dynamic archives, cases which are being worked on, you see the semi or the static archives, and in many

systems in the end, archives are made public under certain rules. That deals with a very fundamental concept of institutional memory of the government. Are old documents destroyed when a new government comes in or is there an institutional memory or a legacy, and is there a right to protect the democratic "heritage"? And how do you organise this in a democratic state? It's not easy but it is worth investing in, it takes thinking about what should be the policy. Are we going to keep everything? In what level of detail? And if not, what are the selection criteria? There is the question of how do we deal with E-archives. If you ignore it then the democratic heritage in the institutional memory will be gone for ever. If it would be the policy to keep everything, and sometimes for investigations I want to see the emails which are being exchanged, you are in a difficult situation.

There are of course time limits, for publicity and access. Is it 20 years, 10 years? Is it 30 years? How long can you retain data? When is the deletion and the special restrictions which may still apply when the archive is made public. In this context the very special problems which arise in middle and eastern Europe, the history is considered for publication, and all the difficult consequences which arise.

There are two famous cases of the European Court of Justice that I want to mention here before I switch to the data protection and public access. First the Hautala case. Heidi Hautala was a member of the European Parliament who simply first raised the question about the arms restrictions policy of the Council. The answer of the Council was very very restrictive. They mentioned

they were in favour of the criteria, one of the 8 human rights criteria, but all the other seven criteria were sensitive and could not be shared with a member of parliament. Then she submitted an FOI claim under the arrangements at the time and eventually this led to a decision of the Court and on appeal, the European Court of Justice gave very firm backing to the principle of the Right to Information being not a fundamental but a very heavy interest and any exceptions must be interpreted and applied very strictly. And then it went on to say that the Council was wrong in rejecting the claim altogether in not investigating which partial solutions could be adopted under the principle of Proportionality. The Court has repeated this in many many cases, one of the last examples was a case in which 47,000 pages needed to be screened and the Court was not prepare to accept a categorical analysis. It said it should be an analysis page by page unless it would lead to an unreasonable amount of work. So that debate continues.

The other case is an interesting Data Protection case but it dealt with an Austrian Act which was basically in its essence Freedom of Information. It was a measure, a tool to put some pressure on the wages in the public sector. They had designed a rather shrewd approach, that the details of the salary of public servants needed to be shared with the counting office and then that office should publish the details in its annual report. You can imagine that was not to the liking of many employees, some senior public bodies did not like it either because they thought they couldn't recruit the staff they needed, in short, it led to a number of cases which came together and the Austrian Act was measured against the data protection directive and the court said, that

although data protection Directive was developed in the internal market, it was by itself a wide concept and applies widely, it also applies to public sector bodies in fact to problems entirely within a member state. And then it went on the give an interpretation of the criteria which the FOI which the Austrian Act need to meet to be aligned with the privacy right in the European Convention of Human Rights.

So there we have two cases which argue on fundamental principles and exceptions needing proper legal basis and proportionality. This was the background against which I dealt with this interface of public access and Data Protection. Two regulations were adopted more or less at the same time with four months between them, but as happens in a real system they were not fully synchronised or harmonised. There were some cross references and some puzzles. So this was seen as a difficult area. Data Protection was new, FOI on a European level was relatively new, how to deal with the interface between the two? There was no comprehensive guidance, there were some bits and pieces so I decided to come up with a paper to explain the interface. And there were some real risks of misuse. I quickly discovered that I was seen as an ally of the privacy against the transparency and I also saw that proponents of transparency were very keen to make the privacy side of the balance as small as possible.

So there was something to gain in helping out how this should be understood and being in these two principles all elements of good government I thought that this would be quite interesting. There was a practice of automatic

rejection whenever personal data were in a document, where they could refuse or blank out all the names because that saves time for one thing. And if it's not pragmatic, it was important because privacy was a fundamental right and so you don't touch that.

We decided to approach the interface from the Regulation on Public Access. There are some reasons for that which I won't elaborate now, but it allowed in my view the best workable analysis. That Regulation specifically states that there should be the widest possible public access. The Court had said that the exceptions need to be interpreted strictly, and then there is the language which came out of the political decision making. I don't think I would have drafted the language in Article 4 (1) b, but it was a ……. And it is absolute grounds for a refusal so the institution shall "..refuse access if disclosure would undermine" (in the original text it was 'could undermine' and we changed this to 'would' which I think is positive) the protection of the privacy and integrity of the individual, (and then it added) in particular in accordance with Community legislation on protection of personal data". Now some thought that the entire of data protection law was now going to be part of this absolute exception and this led to rather automatic denials.

There are different systems. If you put the privacy exception in a relative exception, it would have been different, if you make it a free balance it would have been different, but this is the basis with which I have to work. We decided to read this in a more middle of the road, more in compliance with the existing case law kind of law. This basically means two things. First, the

privacy of the data subject needs to be at stake. The mere presence of personal data is not decisive then would undermine, that certainly would mean a substantial and significant effect not just something marginal. And only then we have to see whether data protection legislation would allow the public access and much emphasis on a case by case approach take all elements into account in individual evaluation.

If we look at the briefly step by step then privacy at stake means that there is a difference between personal data and the right to protection of private life. Protection of personal data developed to cover a wider area and even under the largest interpretations of the European Court of Human Rights it is now clear that the right to private life has a broad scope. It is not limited to the home, it extends to the workplace, it could even extend to public data but I refer to two cases where this is explicitly said Amann and Rotaru, but it is not unlimited. So basically for the purposes of this report we said it is a qualified interest of the data subject. It could be intimate private life, it could be sensitive data, it could be honour, reputation, caught in a false light, confidentiality in a good sense, but a qualified interest. And we specifically emphasised that officials, certainly high ranking officials or political responsibilities do not benefit from privacy in their function. There is a high degree of public interest and that means that it is entirely in line with the case law in Strasbourg that that would not be a valid argument to use privacy against accountability.

Sometimes it is relevant to see whether some of this information has already been made public. You would be surprised. I have looked at cases in which privacy was argued and the same information was more or less available elsewhere. When there is this substantial affection of privacy we very much emphasise the need to contact the data subject for his opinion so as to make the balance work better.

The third element needs to be in conformity with data protection provisions. We have a long analysis in a report which is on my website at www.edps.europa.eu but one of the key conditions is usually whether the disclosure is compatible with the purpose for which this data was collected. That in many cases is based on the reasonable expectations of the data subject when the data was collected. So the key question is under what circumstances were these pieces of information collected and could the person concerned reasonably expect that they would be kept confidential. Then there is emphasis on whether disclosure should be proportional. If is not proportional, then you have to look for a partial solution, look at details, see whether a partial access could be provided and that is the way we have approached this.

We discovered, and this is elaborated on in the report, that you can take two strategic approaches. One is the proactive approach that is, how do you build a system which is transparent, how do you collect information under rules which make sense? In many many cases you do this retroactive when there is a refusal or a complaint etc. We encourage very much to build this

transparency into procedures and we have discovered that this opens up a lot of flexibility in terms of data protection principles not standing in the way. The report has about 12 examples discussed to illustrate this, establish the procedures where very clearly this is announced to interested parties. It can only be lawful and legitimate but by just mentioning transparency and not confidentiality as a default position, then the law works better and the partial access is also mentioned. But some of these scenarios and examples all of which are borderline issues. We do not deal with the easy cases. It's obvious that some exceptions apply and it's also obvious that some exceptions do not apply, but how do you deal with the grey zone, the borderline cases? Well here are a few.

Under standard practice, the CVs of candidates for a public post were taken in a random fashion more or less whatever they contained and then the question arose, "could these CVs be published once the candidate was appointed"? And that was a big problem and it gave rise to a lot of noise. Now in the present approach, there are standards for CVs, how to structure the CV, with relevant information for the selection process, and then it is clearly mentioned in the beginning that the candidate will be appointed and sometimes the shortlist of the candidates which might be appointed will be published. This leads to a much more balanced approach in which you can deal with the various interests as time goes on.

MEP's assistants – Members of Parliament have a budget to employ about 3 assistants, sometimes students. You may have heard stories that some

members do different things with this money and there is an impression perhaps of misuse, so there is a very strong interest in transparency recently of who are these assistants? So there is a list of accredited assistants. Many assistants did not want to be on a list because they said “I’m a student and I want a job but now I’m working for this right wing or very left wing parliamentarian. I don’t want to be on record as absolutely sharing this same political view”. Now that is perhaps a bit exceptional but the parliament decided they would do this and one of the first cases I received in office was a challenge of an MEP assistant against the public list of assistants. To cut a long story short, I thought it was an entirely valid approach, it was acceptable and the fact that this might reflect political views was just part of being an assistant to an MEP in a parliamentary context and the FOI legislation was very balanced, it even provided for a timely challenge that this was a special case and that this person should not be on the list.

External activities of officials – to prevent misuse, corruption, conflict of interests, there are provisions in the Staff rules which make it an obligation to mention external activities of staff. Now that raises some interesting data protection issues, but now the question is, “what about access to the list of external activities?” Well this very much depends on what you consider to be external activities. IF you say anything you do, if you play tennis, if you play chess, we want it all, then that is not really relevant for the job. But if you make the relevant activities for money, influence, possible conflict with the political process, well then there is a very strong interest, and it is not so much about privacy and access could be provided. So here you see the two areas.

Another interesting case is about meetings with companies, company representatives. It was about a competition case in which another company wanted to have access to the minutes and this was rejected for a number of reasons, but one of them was data protection. I think Richard will recognise the use of data protection in areas which the fact that persons meet do not make the data and the minutes personal data protected under the privacy exception. There is a case before the Court of Justice, Court of first instance, which I will mention at the end.

So some examples you will see more, you will see a check list in the report if you are interested on my website.

In conclusion, if data protection and freedom of information are both part of good government, we will probably have to allow this culture of good governance to develop. It needs to be fed, it needs time to develop. But there is only one direction that is the right direction. So I push very much from where I am but FOI is not part of my brief. I have invested in this report because I sometimes deal with the interface and with the data protection part. The ombudsman mentioned this morning that when a FOI claim is refused there is an appeal to Court and there is a possibility to claim, to submit a complaint to the Ombudsman. I am most pleased that the Ombudsman is making very good use of the report that I published last year. He sent me a copy and we do this together with each case in which he requests the Commission to explain his refusal against a background of my report.

Nevertheless I have followed up the report with the Commission. We have analysed in very minute detail what the differences of opinion are, what the consequences would be of a change in their position in simply adopting my recommendations, and we have come a long way. Some months ago I intervened in three cases before the Court of First Instance, it's a possibility I have under my regulation to intervene in a court case, the court needs to allow the intervention, but then this is in these three cases in support of the appellant against the Commission. One of them is the case which I mentioned before on the meeting minutes, and I expect to be involved in the oral hearing on these cases. Any of them will be good for me because this is going to be the first occasion for the Court of First Instance to decide on these two regulations in their interface and if necessary we can appeal this and the Commission and my office have agreed that we will just use these occasions to invite the Court to take a principle stand, and that will be most welcome.

Closing Remarks

Richard Thomas, UK Information Commissioner

The most important person in any organisation is the cleaner, especially a window cleaner. Window cleaners are vital to openness and transparency, and there are still too many dirty windows around. So I stand here proud to be a cleaner. Whether I will sail into the sunset in a boat at the end of the story remains to be seen but I am proud, or I was proud to be a cleaner.

It is my pleasant but also rather sad duty to bring this Fourth International Conference of Information Commissioners to a close. I see ICIC. At the end of yesterday's proceedings I said it was too difficult to attempt a summing up and I find it also too difficult today to attempt a complete summing up. But as with yesterday, various quotes or sentences or phrases struck a chord and perhaps reminded us as to why we are all here.

It was the European Ombudsman this morning who talked of the democratic deficit, talked of elite unconnected, disconnected EU institutions, and I think he was not just talking about EU institutions. He was talking perhaps about

public administrations more generally, and he reminded us that democracy involves choices, but also that all choices must be informed choices.

He also coined the phrase, “Life beyond legality”, pointing out that openness is fundamental to the principles of good administration. Someone else said, “public institutions exist to serve citizens and not vice versa” and none of us should forget that. Peter just now used another phrase to bring together data protection and freedom of information, he used the phrase “The culture of good governance”. Perhaps slightly less elegantly, Andrew Vallance in an otherwise very eloquent presentation this morning coined the phrase, “Private secrecy good, public secrecy bad” – well George Orwell is I am sure still spinning in his grave. Perhaps that could be a new mission statement for my organisation rather than the rather more wordy one which I shared with you this morning.

Tony just now reminded us that access to documents is normally a means to an end, it’s not an end in itself. And I have to say I welcomed what Daniel said this morning after 40 years of experience in the United States, he said very graphically, “Learn from our mistakes”. We are all still learning Dan, but thanks for reminding us of that.

I think I have got the quote right, “FOUO is ‘Phooey’ when it comes to FOIA”. I will have to try and remember what that quote means but remember the significance of that.

Can I also just glance towards the Department of Constitutional Affairs when someone said, “Do remember, FOI cannot be resource-neutral” .

This conference has brought together many themes. One has prompted my favourite FOI true story, bringing together the themes of freedom of information, international relations and football. The BBC a year or so ago went to Sweden and went to the office of the Prime Minister and almost instantly got hold of a hand-written copy of a letter from the British Prime Minister to the Swedish Prime Minister. The letter was very simple. IT was a hand-written letter from 10 Downing Street: “Dear Johan (I think the name was), You were great on the BBC yesterday, Yours, Tony P.S. Thank you for lending us Sven”. Now this was written shortly after England had beaten Germany 4-2 in the European Cup Final, a rare event in recent years, but never mind, but Tony was clearly delighted and Sven of course is the Swedish manager of the England football team. The BBC then went to No. 10 Downing Street after January 1st 2005 to request their copy of the same letter. I think you can guess the ending, No. 10 Downing Street said that the letter could not be disclosed as to do so would prejudice international relations with the kingdom of Sweden. Well that case never came to my office I am rather pleased to say.

We set various aims and goals, we said that we will produce some tangible follow up, in particular. We want to make this a worthwhile enjoyable event, of benefit to Commissioners and their staff, we wanted to involve the wider FOI community. But we said, not knowing exactly what we would be delivering,

that we would produce some tangible follow up. And there will be some follow up, immediately, as soon as possible. We will circulate electronically all the resources that this conference has brought together – the slides which have not been distributed, the papers of presentations, the reports that have been mentioned, the websites, all of these we will share with you, electronically, as soon as possible.

In the medium term, which I hope will not be too long, we will share with you a short report of the conference itself. In the longer term, we will do some thinking. We will think, and this arose yesterday, about the need for some sort of electronic forum for commissioners and perhaps others to share expertise and experience, to swap ideas, to learn all the time from each other not just on occasions like this. We will also give serious thought to perhaps more active participation in International Right to Know Day on September 28th each year. We will give some thought to the challenge laid out before us this afternoon by Helen. Yesterday we heard from one of the speakers about Sunshine Week in North America and perhaps already that produces a model for going forward to be more involved in International Right to Know Day.

I has been a real pleasure to host this conference. We have had participants from over 40 countries. I think that's fantastic. I think that reflects what someone called the 'explosion of FOI regimes'. We have had the crème de la crème of the FOI community so thank you all very much for your participation. I hope you feel better informed, better inspired and better refreshed. I want to extend special thanks to all the speakers, yesterday's speakers and today's

speakers – they have all put fantastic effort into their preparations for their presentations today. I want to thank the hotel and the technical team at the back for all they have done to have absolute first class support, catering and clarity of presentations I want to thank Graham very much for acting as the Chairman of both parts of the conference, thank you very much Graham, but a very special thanks to Dawn Monaghan and her team around the back of the room for a fantastic amount of effort. They have been in contact with many of you in the lead up to this event and they have been really busy. I am delighted with their effort to make this event such a success. And I just note in passing that the team is an all-female team – perhaps we can learn one or two things from that!

Andrew Vallance this morning described a rather curious arrangement with the DA Notice Committee and its relationship with the media as being a very British arrangement. Well perhaps this has been a 'very British arrangement' this conference. We are not terribly keen on resolutions at conferences like this, but it has as someone said, had a literary theme. And I am rather delighted to learn that our colleague Rajan Kashyap from India is going to deliver to us now the poem which he has written I think during his time in Manchester, as tribute to this conference.

Can I invite you now to deliver the 'Poem of the Conference'!

4th
International Conference of
Information Commissioners
MANCHESTER 2006

ICIC: I see, I see!

"Great riches" they said, "lie stuffed in that chest,
Fabulous nuggets from east and from west.

The gems are well hidden, no glimpse can you steal;
A genie stands guard, mark well that firm zeal"

What lies within, you can merely dream;
Dark secrets of state, packed ream upon ream.

"Knowledge is power", that slogan's embossed,
A line read by all; by few ever crossed.

Great minds they struggled, in conference all
To gaze deep inside and pierce that steel wall

All else they contest, on one gaol agree,
The treasure to unveil, for all to see.

Genie overpowered, the mystery is out
of papers, parchments we all know about!

Rajan Kashyap
Manchester, May 23rd 2006