The Privacy Office
Department of Homeland Security
Privacy Office Workshop Series
Transparency and Accountability:
The Use of Personal Information Within the Government
April 5, 2006

OFFICIAL WORKSHOP TRANSCRIPT

Horizon Ballroom
Ronald Reagan Building and International Trade Center
1300 Pennsylvania Avenue
Washington, D.C. 20004

PANEL III
ACCESS TO PERSONAL INFORMATION: A COMPARISON OF INFORMATION ACCESS LAWS

Moderator:

John Kropf

Panelists:

Hugo Teufel
Alexander Dix
Stephanie Perrin
Phil Jones
Lina Ornelas

MR. KROPF: Thank you very much, María. I think your words about democracy and transparency are something that we're going to hear possibly throughout this panel.

I'd really like you to begin with this panel by casting your minds into a little different framework. Think of this panel as an opportunity to take a tour of the European

continent and the North American continent and that up here, we have expert tour guides who are going to lead you around those continents into the world of information access.

And I think like any trip, you're going to see some differences that you'll appreciate and I think you're going to see some similarities that you will recognize. But I think ultimately you're going to come away with this as a real learning experience.

And not only are we going to be looking at North America and Europe, but I'd also like to just mention that in the registrations alone, we have amongst us today representatives from Norway, Uruguay, Switzerland, Belgium, Spain, Germany, Portugal, France, Australia, Japan, Cypress, Estonia, Italy, Austria, and Australia. I probably have missed a few, so I want to cover myself in case I create an international incident to just say all others.

But by now, by different accounts, we -- there are anywhere from 60 to 80 countries and perhaps more that have information access laws and frameworks.

In the very first panel, Marty Abrams mentioned an emerging global process for notices. I'd also like to carry that forward and say there's an emerging global process for the importance of access to government information. It's been emerging now in different parts of the world.

The European Charter in a joint declaration by the UN have said, "A right to access to information held by public authorities is a fundamental human right which should be given effect at the national level through comprehensive legislation."

The World Bank has recently mentioned that information access laws are a critical element to developing democracies.

So with this global backdrop in mind, I've asked our panelists, who I'm going to call them tour guides now, to focus their remarks on two privacy related scenarios under access laws.

The first scenario is access by first-party requesters to information about themselves and the second scenario I've asked is access by third-party requesters and how privacy may be invoked when someone other than the subject seeks information about themselves.

So the way I see this panel is everybody will have the chance to give a brief tour of their territory for the first third and then the second third, I would like to get a good

dialogue going amongst the panel members and then the last third, I'd like to reserve for concise and insightful questions from the audience.

So with that, I will turn the floor over to Mr. Teufel to start the tour.

MR. TEUFEL: Thank you very much and good afternoon.

I don't know about tour guide in my role as Associate General Counsel for General Law at the Department of Homeland Security. I feel more like a smoke jumper, a term that I got from my days over at the Department of the Interior as the Associate Solicitor for General Law.

And by that, I mean it often feels like I'm jumping in with my colleagues from General Law to put out a fire and then get back on a helicopter or plane and fly somewhere else so that I can jump in and put out another fire. And what I had done before government was government contracts.

A lot of what I have been focused on recently has been information law, "Federal Records Act," "FOIA," and the "Privacy Act." And it seems like whether I like it or not, a lot of my time, especially of late, seems to be on employment and labor law matters. But throughout all of those, the "Privacy Act" and "FOIA" have immediate impact and effect on what we do.

So as I understand -- and I apologize, but I had some things that detained me from being here for the earlier panels. And I especially regret not getting the chance to see some of my friends and colleagues from the Department of Justice speak.

But as I understand, Panel II focused or examined the privacy protections provided by the American "FOIA" framework. And I want to build a little bit on that and focus on the American "FOIA" framework and its international implications.

And I'm sure -- of course, I wasn't here, but I gather that somebody has pointed out by now that "FOIA" came into being in 1966 and so we're looking at that 40th anniversary.

And for a change, I'm kind of excited that I'm talking about a law that's actually younger than I am. That's a good thing when the "Federal Records Act," you know, 1950, and "Administrative Procedure Act" and all of those.

The great thing about "FOIA," the American "Freedom of Information Act," is that it starts out with a premise that any person, and that's a key phrase within the act, any

person is entitled to file a request with any agency of the federal government -- now, there are some limitations there -- but any agency of the federal government to ask for records about anything, including whether that agency maintains records about the individual.

And I can't stress that enough. It doesn't matter who you are or where you came from. You can file a "FOIA" request within any agency and seek information from that agency about you or about anything else. And that's very important.

And what does that mean? Well, if it wasn't clear, and, yes, I will belabor the point, it means that citizens of any country may petition the United States government under "FOIA" to see their own records and to request information about various government programs.

In 2004, for example, at DHS -- and we're just one of a number of cabinet-level agencies, not to mention all the independent agencies and the other bodies that are out there, boards and commissions -- in 2004, we processed about 4,500 requests from citizens of other countries. Now, last year, it was about 4,700. Now, most of those were likely over at Citizenship and Immigration Services and related to individuals seeking to see their immigration status files.

"FOIA" presumes that individuals have the right of access to all of their personal information except in specific cases where exceptions apply.

Now, under the "Freedom of Information Act," there are nine exceptions to disclosure and we refer to them as exemptions. Two of the nine exemptions address and protect privacy. Arguably three do because if -- and you may or may not be familiar. I'll briefly mention one and then talk about the other two.

Of the three that I'm referring to, the first is exemption three which deals with statutory exemptions to disclosure and, of course, the "Privacy Act" would be a statutory exemption to disclosure under certain circumstances.

The other two, the first privacy exemption, exemption six, protects personnel, medical or similar files, when disclosure would constitute a clearly unwarranted invasion of privacy. And what constitutes personnel, medical, or similar files has been interpreted broadly to cover information about an individual.

The second privacy exemption, exemption seven, deals with law enforcement records and it forbids the disclosure of information compiled for a law enforcement investigation or proceeding when that disclosure could reasonably be expected to

constitute an unwarranted invasion of privacy.

Congress made a judgment that information from law enforcement files was more sensitive and, accordingly, provided privacy protections that are more easily satisfied. And those privacy protections don't just apply to the investigators. They don't just apply to the prosecutors or cooperating witnesses. They also apply to those who are the subjects of the investigations or those who may be the accused.

For purposes of applying these exemptions, let me state again, because I will belabor the point if it's not obvious, that the citizenship of the information, about whose information is at issue is immaterial. In other words, privacy interests of foreign nationals have been recognized by "FOIA." And I probably will hit that point one or two more times.

Individual privacy is balanced under the "FOIA" against the public interest and disclosure because, after all, what was the purpose of "FOIA." It was for all of us to understand and to find out what the U.S. government is up to.

Even if privacy interests may vary, the public interest is always the same, whether release of the information sheds any light on government activities. On a nearly categorical basis, American courts have held that personally identifiable information about noncitizens such as their alien numbers, birth dates, immigration status, and the like, should not be released because of the potential privacy invasion that release would cause and the fact that there is no counter-balancing public interest. Specific details about individuals whose information happens to be maintained in government files hardly ever sheds light on government activities. And that's the point of "FOIA," government activities and understanding what the government is up to. Our law, therefore, is very protective of privacy.

An example of that would be a case that went to the Supreme Court by the name of U.S. Department of State v. "Washington Post". And for those of you who like to pull out dusty law books or go on line to Lexus and West Law, the cite is 465 US 595. I think it was an early 1980's case.

In that case, the "Washington Post" filed a request to ask about whether certain non-U.S. citizens -- and I think they were Iranian nationals -- identified by the media also had U.S. citizenship or maybe actually had U.S. passports.

The Supreme Court said that the citizenship data satisfied the "similar files requirement of 'FOIA,' exemption for personnel and medical files and similar files, the

disclosure of which would constitute a clearly unwarranted invasion of privacy."

Not only did the court protect the information in privacy grounds, but it also found significant the potential harm that could result to the individual if such information were disclosed.

Under the privacy exemptions in the "FOIA," a wide variety of information has been protected from release. In addition to citizenship information, courts have also upheld protections of information concerning the identities of asylum applicants and related data.

It is important that when considering American privacy protections "FOIA" not be overlooked. It is an important and effective mechanism for protecting individual privacy.

Now, some may criticize the "Privacy Act" for not providing privacy protections for non-U.S. citizens because its -- by its terms, by the plain language of the law, it is limited to United States citizens and legal permanent residents. While this may be true, this is not the end of the story.

The "FOIA," which is primarily a disclosure statute, nevertheless has significant privacy protections build into it for all individuals regardless of citizenship. It is and should rightly be viewed as an important part of the privacy framework of the United States that protects personal information.

Thank you very much.

(Applause.)

MR. KROPF: Well, whether smoke jumper or tour guide, I think that was an excellent overview, and thank you very much, Hugo.

Now we're going to get in our plane and we're going to fly across the Atlantic. We're going to fly east and we're going to land in Berlin. And I believe Dr. Dix is our distinguished visitor from Germany and he's going to give us a tour of German access laws.

DR. DIX: Thank you very much, John.

If you follow me, you will enter, in terms of freedom of information, you will enter a developing country, I have to say. Certainly for the last 36 years when in 1970, the first

"Data Protection Act" was passed in the State of Hesse, the German State of Hesse. It was introduced the concept of the first party or subject access to personal data.

In all "Data Protection Acts" enforced in Germany, there is this Subject Access Right. You can see your own file, your own data held by government. But the concept of third-party access is only very recently -- has only very recently been introduced into the German legal system. And that is something of a revolution, one could say.

In fact, I was in the State of Brandenburg. I was the first data protection commissioner to be responsible for freedom of information. At the same time, State of Brandenburg, in 1998, so only eight years ago, passed the first freedom of information state law in Germany.

And this was result, one could say, of an interesting combination between United States' legal thinking, legal influence and thoughts that came from the Civil Rights Movement of former Eastern Germany. There had been people who have studied the United States and at the same time had been engaged in the Civil Rights Movement in the former German so-called Democratic Republic. And they decided we need free access to files, to government files no matter what their contents are. And they even wrote it into the State Constitution of the State of Brandenburg.

And since then, three more states have followed this example. And most recently, the federal Parliament, federal German Parliament last year passed a federal "Freedom of Information Act" which entered into force beginning of 2006.

So there you are. We are really -- in Germany, we have a lot to learn in terms of how to apply freedom of information legislation and we have much less experience in this field than the United States who will celebrate the 40th anniversary of their "Freedom of Information Act." But still we do have some -- we have collected some experience as yet. Actually, I should add that by summer of this year, there will most likely be a fifth state to pass the "Freedom of Information Act" in Germany. I'm sure within the next five or six years, I'm pretty certain that all German states will have adopted freedom of information legislation.

And right now there's an interesting development to be observed which is typical for a federal state, I could say. I wonder what Stephanie Perrin will add to this experience from a Canadian perspective later on. But once -- in Germany, the idea of freedom of information legislation came from the states to the federal level.

And now once the federal Parliament has passed the federal "Freedom of

Information Act," the states are now thinking of adopting their laws to the federal law which is not always to the benefit of freedom of information because the federal act in some respects is more restrictive than some of the state laws.

So you have a process of, in certain respect at least, of a kind of race to the bottom and standards of openness. And we are fighting heavily to prevent this development taking place, but it's a problem. Maybe the U.S. experience is quite different. But at least in Germany, we're facing this issue.

The states' acts in place address the question of balancing privacy rights and openness issues quite differently. There are state acts which are more privacy friendly than others, but all of them contain balancing clauses. Personal data can in certain instances be disclosed to the public if there is an overriding public interest in seeing these personal data.

But strangely enough, if you look at the same time at the protection of business secrets, trade secrets, the situation is completely different. At least one state act, the Brandenburg "Freedom of Information Act" and the new federal "Freedom of Information Act" protects trade secrets even better and stronger than personal data.

I personally feel this is probably even a constitutional issue because there's no good case to give stronger protection to business data or trade secrets than to personal data. But that's the law at the moment. And I wonder what the courts will make out of this. It's a very interesting question.

I think that there are -- in fact, there's a different federal law governing access to environmental information and there you have a balancing test when it comes to business data and trade secrets.

Now, I wanted to make two additional points to give you one practical example from my own jurisdiction which is at the moment still before the courts and which has a kind of international link.

A journalist in the City of Berlin one day made an application under the new law to access the schedule, the official agenda of the governing Mayor of Berlin. Now, he only wanted to see the official dates and meetings the mayor had in the past. He was only interested in the past official dates and meetings. The governing mayor turned this request down.

The journalist came to us as the Freedom of Information Commissioner and we

supported him. We said there's no legal ground for the governing mayor at least to in toto refrain from disclosing or reject the request for to disclose the schedule. And he then went to court because we don't have the power to order any public agency to disclose information.

So he had to go to court and he lost in the first instance where the court -- the first -- the court of first instance gave a very strange reasoning. They said, well, the governing mayor's agenda is not a file in the sense of the act, which I couldn't quite make out what that meant. It's a very technical argument. And now the journalist appealed this decision and it's before the court of second instance. But from an international point of view, it is interesting to note that the President of Mexico, the Prime Minister of Canada, and even George W. Bush, at least in his capacity as Senator -- Governor of Texas, if I'm informed correctly, had to open up their official agendas due to freedom of information requests. But the governing Mayor of Berlin still refuses to do so. So that is somewhat strange. But the legal question is still unresolved as I said.

Secondly, another interesting point of comparison is the scope of the German freedom of information law. The German law expressly excludes intelligence services as a whole from the scope of this freedom of this information law.

Now, this is particularly interesting in comparison with the U.S. situation where you have the Federal Bureau of Investigation coming under the "FOIA" scope, although certain exemptions obviously will apply and quite often may apply, but the scope of the law covers intelligence services whereas in Germany, it does not.

So you see there's a lot of work to do in Germany. And I pass over to my -- John Kropf and my Canadian friend.

MR. KROPF: Okay. Well, thank you very much, Dr. Dix, for that overview.

And now we are going to hop across the Atlantic the other way again and we're delighted that Stephanie Perrin could join us from the Office of Privacy Commissioner of Canada.

Stephanie, the floor is yours.

MS. PERRIN: Thanks very much.

And I'm very sorry that Harry Hammitt isn't here this afternoon because I was going to appeal to that accelerated forgetting clause that Mr. Huff was speaking of this

morning.

I was one of the first access to information and privacy coordinators in the federal government in Canada after the law passed. But for about the past -- that was in 1984 to '89, I think it was -- but for about the past 17 years, I've been largely focused on privacy.

So if any of you have any hard questions about recent case law, I'll have to take it home and consult my colleagues, I think, seeing as how Harry is not here.

Our laws are very similar to those that are in the United States. The "Federal Privacy Act" passed in 1982 as did the "Federal Access to Information Act." We call it ATIP in Canada.

The major difference that you will note right away is that each office has a separate independent ombudsman-like commissioner who hears complaints, investigates, has audit powers, can go in, and periodically we audit government departments to see how they're complying. We publish an annual report.

While we do not have binding powers to force the government to release information, the effect of reports to Parliament and testimony to committees and the annual, of course, "Privacy Act" report does tend to push people along.

Now, the information commissioner has, I would argue, a much harder job than the privacy commissioner because we have many of the same situations in Canada that I heard described this morning.

The delays are becoming, I would say, endemic and the information commissioner's response to that has been to subpoena heads of agencies to come in before him and testify under oath as to why this was happening. It hasn't gone over well in Ottawa. I think I can with all due diplomacy say that there's a certain amount of tension in town over this practice.

His comments about how the "Access to Information Act" needs to be revisited, though, have been heard by the Comments Committee that is responsible for oversight of both of our offices and they have indicated a willingness to entertain revisions to the act.

The new government -- I was on a plane when the throne speech was being read yesterday, but they have indicated a desire to increase federal accountability and part of that will be revisions to the "Access to Information Act" in the name of transparency. What that's going to look like, stay tuned. We don't have a picture at the moment.

There was a bid in the fall of this year, a former Supreme Court Justice was named by the Justice Department to do a study on whether it would be advisable to amalgamate the privacy -- Office of the Privacy Commissioner and the Office of the Access Commissioner.

In fact, there's quite an interesting discussion about that reflected in his report which is on line. If anyone is interested, I'll be happy to take your card and provide the URL.

But on balance, it was determined that there was a healthy tension between these two offices over some of the very issues we've been discussing. It's good to have a champion for access disagreeing with a champion for privacy while the issue is sorted out because things do become very complex when it comes to the public's right to know.

Now, we have an addition to that. Those bills passed in 1982. In the year 2000, a new "Privacy Act" for the private sector passed, PIPITA. It is up for review this year in 2006. There is a mandatory every five years review of that bill.

Unfortunately, there was a one-time three-year review of the other two pieces of legislation and it was reviewed by Parliament and there were recommendations made in a volume called Open and Shut. And sadly nothing ever happened after that.

We hope that the annual -- the every five-year review of PIPITA will continue because these laws do lose their relevance as the techniques change. You know, these still talk about records in file. We're not talking about data monitoring. It's a bit different. Search engines weren't even dreamt of back then.

At any rate, in addition to the federal laws, I think it's important to note that we have provincial laws in 14 different federal -- 14 different provinces and territories. Each one has some kind of an oversight agent. Sometimes they're called ombudsmen. Sometimes they're access and privacy commissioners.

They have both roles. Sometimes they have binding powers to force the government to disclose. And that group meets twice a year to discuss common issues. It's very interesting how the different issues arise in the different jurisdictions.

The law itself in the provinces tends to be an amalgamated law where you have one freedom of information and privacy law and you have a right of access that is slightly different if you're an individual.

In Canada, we are calling in the Office of the Privacy Commissioner for review of the "Privacy Act" because it is so old, because there are many things that don't work, because, frankly, it is embarrassing, at least we feel, an embarrassment in the federal government that the private sector has to meet a much higher standard in the new private sector law than the government does.

And I won't go into the litany of problems, but it's rather similar to the issues with the "Privacy Act." Consistent use is the term in the federal government for once you get it for one purpose, you can use it for many other purposes, as opposed to the private sector law where there is a reasonable person test.

I wouldn't like to infer in any way that or imply in any way that bureaucrats are not reasonable people, but there does seem to be a tendency once you've got the information to use it for other uses that everybody all agrees are reasonable or at least consistent. So that's one of the things we will be calling for.

We will also be calling for -- and a paper on this subject will be up on our web site very shortly. It's just in translation now -- we'll be calling for an expansion of the right of access and full rights to go to Federal Court under the new law. Basically that there have been two order and council amendments providing rights to non-Canadians, but you still have to be in Canada to exercise your rights under the "Privacy Act."

So we ran into a little bit of a road block when we were dealing with the PNR issue, the passenger name record issue, and we had to get agreement from the government agency involved that they would indeed honor Europeans' access rights. It would be far better to just open it up and provide privacy rights for everyone.

Nevertheless, as in the United States, the full suite of protection powers and nondisclosure applies. It's just the right of access that is different.

Now, if I still have time, there are a couple of issues that I think are interesting. We had discussion this morning about disclosure in the public interest. And one of the things that frustrates our office is very often information is not disclosed and the "Privacy Act" is cited as the reason for it.

So you will also see shortly on our web site a rather mildly-written fact sheet explaining why the particular agency has the discretion to release personal information when it is in the public interest. They are to inform us. We can then, you know, express our dismay if we think this isn't a genuine public interest.

But it has been cited in a variety of cases, usually where the public interest is -- I shouldn't say usually, especially not in the record -- but let's just say that we want everyone to understand that when there is an emergency and it's life and limb at stake, it's quite legitimate to cite a 2-M to release the identify of an individual.

We had it raised, for instance, during the terrible Tsunami that hit where, you know, it was impossible to find out where people were. And, you know, frankly, we can find ways of working around these situations when they do occur.

One of the issues that causes some debate in Canada, of course, is the identification of dangerous offenders when they leave prisons. It is now accepted that dangerous offenders in certain categories, we can notify where they are being released. So that's one issue.

The other one is an issue that I think -- the second issue, I think, is well known to many in this room and that is the issue of accelerated or -- not accelerated -- but much broader diffusion of court information.

There are many tribunals of an intensely personal nature such as disability pensions, many things under the federal employment legislation where there's an interest in having an open court record when these cases are being heard. They're putting them on the internet.

We, of course, would like to see them not put on the internet or put a redacted version on the internet and put that threshold of work between those who feel they need to know this.

We are working towards a policy. The Canadian Bar Association has a good paper on this subject and we're hoping we're going to see some movement on that.

We receive a number of complaints in our office about it from anguished people whose gory details are being put up the internet.

And the last one is a far more difficult problem that I don't think anybody is going to solve any time soon and that is the privacy of groups and privacy of individuals with respect to data that has been de-identified, distributed to the public as statistical information, and then re-identified.

Now we've dealt with this issue in the direct marketing context for many years.

Oscar Gandy has written about in "Panoptic Source" back in about '94, '95. However, it's getting more complex. Our own statistics Canada, which is a federal issue and I'm looking at it in the context of federal policy, releases and sells a great deal of detail of information. It has been de-identified. But enterprising data brokers, statisticians, and universities pick it up, reapply it to categories of people.

And it's probably more accurate than credit records are in our country with all due respect to anybody representing the credit business here. You know, if it's 85, 95 percent accurate, it might as well be personal information. And, yet, arguably it's not personal information.

So this is a problem. We have received a few complaints. If anyone has the answer to that, I'd like to know what it is, please, because I see this as a coming confrontation, not just between the information commissioner and the privacy commissioner, but between academia and folks that are fighting for privacy.

And the allies, I suppose, on this side are those from particular designated groups, whether it's, you know, racial groups, poverty, discriminated groups, patient groups with particular diseases, people who've lived near known polluting entities such as polluted rivers or nuclear energy sites, you name it. There's a wide variety of applications to this kind of rich data set and it's going to be the issue for the next ten years.

So on that cheery note, I'd be happy to take any questions later.

MR. KROPF: Thank you very much, Stephanie.

And I know at one point during your presentation, you posed the question whether or not bureaucrats can be reasonable, and I certainly think you would pass that test more than -- quite easily.

MS. PERRIN: Some would argue with that.

MR. KROPF: But thank you for that tour of Canadian information access.

And we're going to get a little jet-lagged here and fly back across the Atlantic to land in the UK where Mr. Phil Jones is going to give us a tour of the rather still new UK information access law.

I think you've just celebrated your first anniversary? The floor is yours, Mr. Chairman.

MR. JONES: Thank you very much, John.

I calculated I'm the 22nd speaker from the panel. The fact that some of you are still here says a lot about you, but it does also mean it gets pretty hard to think of anything new or interesting to say. So I'm apologizing in advance.

You will note that I'm designated as coming from the UK Data Protection Authority. That is, in fact, true. But we're also the UK Freedom of Information Authority as well. So we're called the Information Commissioner's Office because it sounded like one of those names that's a good name at the time because it covers both aspects of our role. The only difficulty is nobody understands what the role really is. They just ask us for information.

(Laughter.)

MR. JONES: But the UK -- our office, therefore, has responsibility for data protection across the UK and freedom of information across the UK except Scotland which has its own freedom of information commissioner for complex reasons, political devolution which I won't trouble you with.

The UK has only heard state protection legislation, that is legislation applying equally to the public and private sector since 1984. Our office under an earlier name, therefore, has had 20 years' experience of enforcing data protection rules, rules which require those that use pertinent information for business purpose to be transparent to ensure data quality, to adopt appropriate security, and to provide individuals on request with copies of their personal information.

And, therefore, it's true that UK citizens have had a right to request copies of their personal information which government bodies use to determine matters such as entitlement to a welfare benefit, and they've also had the right to challenge the accuracy and relevancy of that information.

But there's two points. First of all, you don't have to be a UK citizen to exercise that right. You don't even have to live in UK and you don't actually have to be in UK. You can exercise that right of access from anywhere in the world. And our privacy law, therefore, applies regardless of citizenship or domicile.

And the other point I wanted to stress is that it's not just government bodies. Our law has always applied equally to private sector organizations, many of whom the big credit reference agencies, the big information brokers, the big banks also hold extensive

amounts of information about individuals.

Now, it is true that we are very much novitiates in the area of freedom of information. Our law was only passed in 2000. And access rights only came into force 15 months ago. So we're at a very early stage.

There's a broad right of access to information held by government and other public bodies and bodies that are carrying out public functions, those complex definitions of where the edges are.

But crucially the law provides where the information requested constitutes personal information that it should not be released where to release that information to a member of the public would contravene data protection law.

And so what that actually -- it also says quite logically that if somebody made a freedom of information request to you for their own information, that is then to be treated as a request under data protection legislation is long existing right to your own personal information.

Now, what we're talking about now is where somebody makes a request that's either directly about information about somebody else or indirectly, you know, that the information they request would include information of others, about third parties.

Now, one of the most interesting things about this is that one of the things that we've discovered is actually determining the edges of what's personal information or not is not that easy. And we've had 20 years of it, so you'd think we'd have sort of got it buttoned and sorted out.

But actually what had happened in the past is that many organizations have been prepared to treat information as if it was personal if it did need to be given proper care, proper security, and they hadn't bothered too much about how near the margins it was.

But under our freedom of information legislation, it becomes very crucial because, as I said, if releasing information releases personal information about another person, then there has to be a judgment made whether that release of information would be in breach of data protection law, broadly whether it would be unfair to that individual.

So the big decision about deciding exactly where the edges of personal information is and that's not always straightforward. And then after that, there's a decision to make about whether if it is personal data, is it all right in those circumstances to release it.

Interestingly, as I said, people always pitch the interesting bits if you come at the end. I thought I was doing really well. But Stephanie got to my most interesting bit and I got really close. I was only one person away.

(Laughter.)

MR. JONES: In UK, as I'm sure in many jurisdictions, we've always had quite strict rules, very strict public policy about releasing information that's released from things such as censuses or other statistical information and very crudely -- in UK, I think it's the "1911 Census Act" makes it a criminal offense to identify somebody from census data, to seek to identify them, and actually even to purport to identify them, to say you've identified them.

And we've had big debates about releasing small area statistics for researchers and there's all sorts of technical measures to make it difficult to enable somebody to authoritatively identify an individual from those raw records.

And the broad approach that's being followed under census legislation and to do with the release of certain things such as health statistics is that if there's the slightest risk of releasing personal information, the public policy has been to err on the side of caution and if there might be a risk you could reveal something to somebody, then you wouldn't do it.

Now, the problem is, and it probably reflects the need to revisit even the "Freedom of Information Act" and the existing exemptions there, the problem is many people face -- public authorities faced with releasing statistical information, which they're uneasy about revealing, their first aim and perhaps, you know, their main aim is to see if they can claim it's personal data and then they can go off down one road.

In one particular case, it related to somebody asking for details of the incidence of childhood leukemia in a very narrow geographic area in Scotland, very small ward sizes. And they were very uneasy to do it. It's a very difficult decision because whether somebody can link to an individual depends on what the people you give it to know. And you don't know what they know.

And so it's this big problem about there being a real clash here between the public policy such as being built upon trying to seek to ensure the people did confide in census officials, did go to see doctors, et cetera, on the one hand and an equally powerful public policy towards transparency on the other. And I actually think it's quite a difficult era,

but a new era for us at the moment.

When we get on to deciding whether to release personal information -- and this is where I was intrigued to listen to the American experience where, as I understood it, you know, you sort of -- there was some obligation to ask the person. You had to go and try and get permission from the person next door if you wanted information about them.

The decision actually doesn't involve the individual. There's nothing in the law that suggests that it should. I mean, it could be, but there's nothing that says you have to.

But in very broad terms, the sorts of considerations that you would take into account is whether the information is about somebody in the public or private capacity. And it means that we're more likely to take the view that those who have a right to say over how public bodies spend their monies, et cetera, should be subject to a greater degree of scrutiny.

And that would mean that the details of the expenses of an elected representative such as a Member of Parliament or public official such as the information commissioner or grants for public funds given to farmers should be related. On the other hand, grants given to those who are hard up from a social (unintelligible) enable them to purchase domestic essentials such as a (unintelligible) would tend not to be.

But that would be on the grounds of whether or not it was fair in respect to data protection legislation. And the assumption would be that as it were with power and place and position, particularly in a -- in your public or working capacity, the more senior individuals certainly are properly subject to a great deal of scrutiny.

Just very quickly to finish off, the other thing our legislation tries to do is it tries to encourage organizations to review all sorts of data that they've got and then come up with a publication scheme which is a broad explanation of the sorts of information they will routinely make available and then to actually go ahead and publicize that information.

And the idea being to encourage them to be more open, but the quid pro quo is that if the stuff is available through ordinary measures on a web site, et cetera, then they don't have to respond to an individual and specific request.

So if you'd like, the more they get out there anyway, the less pain they have of having to respond to individually constituted requests.

So if somebody makes a specific request and it gets denied, they are required by

the law to go back to the public authority and demand that there be a review of the decision and there's obligation to review that decision.

If they're still dissatisfied, they can complain to our office. We then make a decision. When we've made a decision, either party, so that could be the public authority or an individual requesting information, can appeal to an information tribunal which is a specially constituted tribunal which will then make a determination. And ultimately there is also an appeal to the high court.

Now, the past few months, there's been an awful lot of appeals. Most of them have been from individuals and most of them have actually been from where we have upheld the public authority's decision. It means it's a very busy time at the moment.

I think what we hope is that over the next couple of years, as we get more experience, but also in the light of decisions made by the information tribunal, that it will be -- we'll move to a position where there should be less need for regular decisions of that sort.

So, finally, 15 months, it's been interesting, but I think we're very, very well aware of how new it is.

And the final point is our office quite properly is fully subject to both laws that is has responsibility for and that means that I personally have handled individual subject access requests and also freedom of information requests.

Thanks.

(Applause.)

MR. KROPF: Thanks very much, Phil.

I am particularly struck by what you started out with which is to say that virtually anybody can file a request for information, citizen or not, anywhere, any place. And I'd like to maybe get back to that point during our discussion.

But now I think we're going to take our last flight back to Mexico where I think that's going to be a very nice place to land and hear our final panelist, Ms. Lina Ornelas, who's going to speak on the Mexican access laws.

Lina, the floor is yours.

MS. ORNELAS: Thank you very much.

First of all, I want to thank Maureen Cooney for the invitation to participate to this workshop and, of course, to John Kropf for all the kindness.

Well, this is a very good opportunity for us to share with you our experience in terms of data protection in the framework of our law which is a law of access to information.

In Mexico, we have several regulations that are aimed to protect privacy and -- but they are in different laws. We have some in the Articles in the Constitution, in banking and tax laws, intellectual property laws, et cetera. We have also the no-call lists or do not call lists that they are going to be applied.

Deleted: (unintelligible)

But in 2002, we have our own "FOIA." And within this law, we have a chapter on data protection. Let me tell you that it's only for the federal government. It's not private -- private sector is not covered by this law. So only the executive agencies and the legislative and judicial branches and the autonomous entities created by the Constitution are covered.

And one of the main objectives of our "FOIA" is not only to give access to information accountability and archives, but also to guarantee the protection of personal data. And that's very important because we had the regulation that really strongly -- it's aimed to protect this information and to give right to citizens to ask for their own personal information.

So just to give you an idea, the time for answering and access to personal information data is shorter the time than access to information of the government. So in ten days' time, you can get your own information whereas in 20 days' time, you get information about the government. So -- because it's considered a fundamental right, the right of access to your own information.

So we have a definition of what is considered an individual information or personal data. And we have all those categories and some other analogous. So we have -- you know, the government uses information, personal information for different activities and for complying the law. So this information is considered confidential.

The category of information that is in the archives of the government is considered privileged and it's like that for 12 years whereas confidential information about persons is

considered like that during the life of the person. So we do not give access to personal information unless there is consent of the individual.

The government asks the owner of the information if he doesn't answer or if it can't be found, for instance, so the answer is negative. So we have a procedure for that.

And we have had several cases of public interest, balancing tests and things like that because we as public servants, we have a lot of personal information which is public like our salary and things like that.

But people want to know more than that, like medical files of public servants and how many children you have and things like that. So we have -- well, the commissioners have some different cases where they have applied like a public interest test.

Okay. So I'm going to be quick in this slide. The President said if I -- it's only an institute for the federal Executive Branch. We have more or less 240 federal public agencies. So have to -- we have a lot of work. And we have to make them comply with the law and we issue regulation for them.

Our tasks, as she said before, is to resolve appeals presented by individuals. And, of course, we guarantee access to personal data including the possibility to replace, rectify, complete, or correct such information.

And we have recommendation actions to the comptroller minister because that's the only thing we can do. We cannot do something different. But our resolutions have -- they are very powerful because you make public that an agency is not complying with the law, they react very well.

So what kind of or what type of personal data does the Mexican government have or possesses? Well, it doesn't work very well, but -- information related to the compliance with laws and regulations, tax collections, population census, et cetera, et cetera, and also have financial education and social assistance services among others.

So as you know, we also have a lot of archival problems, so we are very concerned about that and we are issuing some regulation to keep all these archives in a correct manner so they -- the people can access to their own information.

So how do they treat that information? Personal data is obtained according to that -- what government can do specifically permitted by law and cannot be disclosed or transferred except for the purposes or objectives for which is was collected.

So the government cannot do something different that the law says. Therefore, direct marketing or personal data that the government has is not allowed in Mexico.

And I'm going to give you some numbers quickly so that you can have an idea. While receiving more than 126,988 requests of access to public information, that's from 2003 up to date. So we also received 10,000 requests of access to personal data.

So it's only -- it's one percent. Although the appeals is one of each five is concerned to personal data and confidential information, we have received 5,000 appeals and 1,000 of them are related with personal data, especially with access to file and medical records as the President said before. So people can now have access to their own medical file.

So we have issued some regulations. They are aimed, of course, to regulate this, guidelines regarding the procedures to access to information, et cetera, et cetera.

But something I wanted to share with you is that our law has to comply, let's say, with internationally recognized principles, principles of data protection such as lawfulness, quality, access and correction information, security, custody, and consent. The law and regulations are based upon the OECD models, European directives, and the principles of APEC.

But how can we tell people that they can use their rights to access to their own personal information? Well, we have created a system that we call Person System which people can use. We have 755 different personal databases now. We have a register. So we tell the government that they have to look in their archives to find what kind of personal data they have. So they told us up to date that they have 555 different databases for different purposes.

And we have a list and that list is public through this system. Even you can check it out through internet. And what we do is that we put all the federal agencies and you can choose one of them and you can see all the systems they have and what kind of personal data is there.

The federal government has reacted positively to the necessity of protecting personal data and seeks to create a culture of protection thereof through media campaigns. And, for instance, for the privacy notices, we use posters or things that people can understand. And we also seek to pursue this and exchange experience through different participations in international meetings and stuff.

But this system is very interesting because you can see what kind of data the government is collecting and what are the purposes, who is responsible for that database, and for how long they are going to keep it. And people are using it and it's, let's say, the beginning of a culture for access to information.

We also have the problems that have been said before about extension of rights, but we are trying to apply this public interest and test and balancing privacy versus openness.

So thank you very much for this opportunity to share with you what are we doing. Thank you.

(Applause.)

MR. KROPF: Thank you very much, Lina.

And I meant to point out that there are handouts of Lina's presentation on the front table as you leave. So if you're interested, there's a limited number of copies, but there should be about 50 out there for you if you're interested.

At this point, I would like to now get a bit of a dialogue going with the panel and then have us discuss some issues. And then following that, I'd like to take some questions from the audience.

But I'd like to maybe get things going and talk a little bit about -- we've heard the word consent mentioned occasionally. It was mentioned in the second panel about when you have a third-party request, if you go out and get the consent of the subject of the request or not.

And just taking kind of a casual look at -- I notice in the laws of Canada and Germany, they both have extensive provisions in their law about needing to get consent. But I wanted the panelists to comment on what are the requirements or standards. Is there a process in place where you would actively go out and seek consent or not?

So I will throw that out, the first question.

MS. PERRIN: I think this comes under the category of one of those questions I'd rather throw to Harry Hammitt because I'm not entirely certain what the latest cases have found on this.

One issue that has been a problem since the beginning of the act is situations such

as harassment investigations where you have an investigation where individuals were assured that they would give testimony in confidence and, in fact, then the individual who is the subject of the harassment allegation comes in and wants to get the testimony of all of the witnesses.

The privacy commissioner -- and this is one of these healthy little discussions between the privacy commissioner and the information commissioner -- the privacy commissioner has taken the position in the past that the greater balance is on the side of the individual who is the subject of the investigation and that the opinions given by a public servant which are not considered to be personal information in the context of giving an opinion or judgment while working for the federal public service, that's not considered to be your personal information.

So that should be, therefore, released to the individual who it's an opinion about, if you follow my twisted language here. So I think that's pretty well a given.

Where you have a voluminous request for records and let's say you've got -- I don't know -- 10,000 pages of records being requested on a large file, routinely the agency will go through and exempt the personal information under the exemption for personal information which cross links between the "Access Act" and the "Privacy Act." It referred specifically to the definition of personal information in the "Privacy Act," and it says you can release it under that -- or rather exempt it under that.

And then, of course, the requester will come back and say can I have all of the stuff that you exempted. Why don't you go and consult them. And in some cases, organizations will indeed, if it's a fairly small category, consult the individual. If it's voluminous, I don't believe they're under any other obligation to do that, to take that on.

MR. KROPF: Phil.

MR. JONES: Can I just start with under our data protection legislation? I mean, data protection and a lot of things would be easier if human beings weren't social, but life would be pretty boring.

The problem is that a lot of personal information is actually wrapped up with other people's personal information because life is like that and that's what families are.

And so there are provisions in our data protection legislation about what you do when personal information that is about me also includes personal information about other people to whom I'm closely associated.

And under our law, you've actually got to consider whether the person concerned has been asked for consent and whether they have actually refused consent. If they consent, you're then obliged to pass the information on. But even if they don't consent, it still may in all the circumstances be the right thing to pass that information on regardless. So it's actually quite a complex decision there.

Now, under freedom of information legislation, there is nothing specifically says that a body has to seek the consent of an individual in those circumstances, nothing to stop them doing so either. But, again, taking a lead from our data protection legislation, even if they said no, this wouldn't necessarily constitute a conclusive reason not to provide the information.

MR. KROPF: Dr. Dix.

DR. DIX: I can add a little bit to what Stephanie and Phil have said very much in the same line. Consent is only one possible justification for disclosing personal data under "FOIA" legislation in Germany. There are situations where even without consent, personal data may be disclosed. The major case being public servants.

And Stephanie has said public servants, the name or the title or the function a public servant is carrying on is not considered to be personal data under Canadian law. It would be personal data under German law, but it would be personal data which can be disclosed and must be disclosed if a request is made.

So as long as the information only concerns a core set of data relating to this public servant.

There are other information, for instance, under the Berlin law which is the most -- probably the most freedom of information friendly piece of legislation in Germany where privacy is the most limited in this balancing, delicate balancing provision.

The fact that a citizen has, in fact, applied to a government agency to receive anything or has made an application not to mention for what or if he's subject of administrative activities in some case, in some sense, this very fact can also be disclosed, but nothing else, nothing beyond this very general point.

And, again, there is a proviso if in such situations legitimate interest of the data subject would be violated by disclosing this information, then again, it has to be withheld. So you have a kind of balancing test both ways which can be rather difficult.

And a new federal freedom of information law explicitly refers to sensitive data. Under the European data protection directive, you know that health information, information concerning political convictions, even -- well, sex lives, ethnic origin, this kind of information may only be disclosed under German freedom of information law with the explicit consent of the data subject. That's a specific proviso in the German federal law.

So that's a little bit maybe from the German perspective to this issue.

MR. KROPF: Any other takers?

MS. ORNELAS: Yes. Our federal law is an access to government information and it clearly states that, okay, people that owns their own information cannot -- that the law doesn't solve the problem of how to deal with access to personal information from third parties.

So the regulations that the person (unintelligible) in Article 41 and it says that when a department or entity which is a request for access to a file or to documents containing personal data and the committee -- there's a committee that decides within the agencies how to release information -- if the committee considers such as pertinent, the department or entity can request the holder of the information to approve its delivery and will have ten workdays to give it. And the silence of an entity shall be deemed as a refusal, as I said.

So first of all, if it's not the first party, the owner of the information who asks for it, then you have to look for the owner, ask for it. And if you don't find the file or they don't answer, the silence is considered to like a refusal.

So -- but still we have had very interesting cases. Like, for instance, a person asked for the whole pictures of public servants in different federal agencies. So he wanted the whole pictures and the commissioners decided not to release them because there was no public interest, a clearly public interest, because of the image of a public servant is not considered to be related with accountability, let's say.

Of course, high-ranking commissioners are on web pages and they are -- if they are public figures like ministers or honored ministers -- well, they are public figures and stuff, but the picture of the secretary -- and it was a database, a complete database.

So once -- you collect the data, you collect the picture for a very clear purpose,

which is to identify yourself in a building or to make -- do your work or whatever, but not to release it to everyone.

So that was one of the recent cases that the commissioner solved.

MR. KROPF: Okay. Well, I think I'd like to try to move on a little bit to connect both the morning and the afternoon, so that all just makes sense.

In the morning, we did notices. And I view the notices as the front end of the process. It's in essence the government making a promise to the public saying we're going to collect information on you and here's what we promise to do with it and here's how we're going to handle it for this purpose.

And I look at this panel and the last panel as the back end of the process. This is a tool of accountability or transparency and it's the public's opportunity to then ask the question, well, government, did you live up to your promise, did you do what you said you were going to do in the notice and now this is my chance to find out by filing an access -- information access or "FOIA" request.

And I'd like to just open it up for your views on how effective you think your information access frameworks are in accountability and transparency in this process.

I'll start with anybody who'd like to take that.

MR. JONES: I'll take it first.

MR. KROPF: Please.

MR. JONES: Because I've been with our office for quite a long time, it doesn't mean that occasionally -- you think the world hasn't changed very much and you take stock and you find that thankfully some things that you used to have to deal with a lot, you're not having to deal with.

Certainly I think that the individual right of access to their own records has made a marked difference to the way that everybody from doctors to other -- and other professionals hold and what they decide to say about somebody because what they don't know is if that person might be a person who requests to see a copy of that information and that, I think, is actually quite a powerful discipline.

So I think the individual right of access has caused people to be more careful about

the quality of information that they record about individuals. And if that means that people are more careful what they put in personnel files, medical files, et cetera, then I think that's very much a good thing.

We haven't been dealing with FOI long enough, I think, for us to be -- to come to any conclusion regarding FOI.

MR. KROPF: Stephanie.

MS. PERRIN: I think that you're touching on -- and I don't mean to broaden this out to something -- an ungovernable scope. You're trying to wrap it up.

But one of the problems that we are dealing with quite a bit in our office is the general level of ignorance of the public about information flows.

So, for example, under the private sector legislation, we've had a couple of complaints since you passed your "Patriot Act" when people discovered that their banking information was in the United States. And a couple of brave banks had gone forward and come up with what were really, we felt, quite good privacy notices saying we do this with your data, very extensive list.

If you've been at this as long as some of us have, you remember those original notices say that we'll gather every bit we can and we'll keep it forever and even after you cease doing business with us.

And we've now got to really quite decent privacy policies. But then when they say this -- because the public has been blissfully unaware that banking records have all been cleared in the states for, I don't know, 25 years, 40.

I mean, it's really one of the pushes for the original issues over transporter data flow was remote data processing driven by the banking industry. So hello. Knock, knock. And I don't wish to be disrespectful of the public. It's our job to educate them about data flows.

So as we creep forward providing more information. And we, too, have a director of information, both personal and general, in the government department, but you'd really have to be a person without a life to have gone through that directory in any great length. It's up on the internet now. Maybe a few people at least can cruise it, but it's a great big, thick tome, pretty boring.

So that's not a good vehicle for getting the public educated. And one of the challenges we're looking at in our office is how do we get people who understand what is happening. One of the issues that we're debating right now is what's decent notice when we're dealing with things like RFID readers, when we're dealing with video cameras hidden or otherwise.

Deleted: (unintelligible)

We understand there are certain locales where video cameras are hidden. What are those locales and which ones are acceptable and which ones aren't? You know, what kind of notice do you have to give people and how much is on that notice? And do you have to list the 40 agencies that can routinely come in and access those records without any other kind of written authority?

So not to sort of throw things out at the end of the afternoon, but I think that's one of our biggest challenges. It doesn't fit on a short (unintelligible).

And the other issue is if you rely only on notices, you're going to trivialize the issues so that people will -- it will be like the cigarette one. And in Canada, we put big scary warnings on the cigarettes. It doesn't seem to be stopping anyone from smoking.

MR. KROPF: Dr. Dix.

DR. DIX: Adding to what Stephanie has just said, I'm still fond of short notices, but there are obviously limits to simplification, the first thing one has to keep in mind.

And, secondly, I think freedom of information is a much larger issue than just notices. Notices are addressing the question of how personal data are being processed. What happens to personal data you are giving to the government or to a private company whereas freedom of information goes far beyond that. It -- David Sobel, I think, phrased it this morning the flow of information between government and citizens is changing and being reversed to a certain extent. That's the intention at least to freedom of information laws. It's a question of power in the end and goes far beyond simply the processing of personal data or merely restricted to the processing of personal data. It is a bigger task.

And to find out how effective this legislation is, with all respect, this is a question either of friends from the United States with 40 years' long experience or our Swedish friends with 300 years' experience, are far better equipped to answer this question. We only have eight years' experience.

MR. KROPF: I should have mentioned -- I meant to in my opening remarks -- that Sweden was the very first country in 1776 to actually put into its Constitution an

information access law.

So thank you for bringing that to our attention.

Hugo.

MR. TEUFEL: Seventeen seventy-six, great year.

(Laughter.)

MR. TEUFEL: I had to say that. I am with the U.S. government after all and that year has some relevance to us.

Accountability and transparency, I'm not sure how we're using them and we can be using them in a lot of ways. But as I'm a government practitioner and not an ombudsman or a privacy or information advocate, I think about accounting and transparency as follows:

With respect to accountability, we have a mature administrative process. We have mature administrative processes here in the United States that allow for resolution. And if that doesn't work, there is always avenue to the courts of the United States under the "Administrative Procedure Act" or other laws or the Constitution.

With respect to transparency, again, my client is the department and the United States. And so, you know, I'm always trying to advise clients to be careful what they put in writing when a phone call would better do or a face-to-face conversation.

But transparency as a citizen, as a taxpayer, transparency means a lot to me because it is important that the citizens know what it is that their government is up to. And, of course, this is Washington, D.C. and nothing ever really remains secret in Washington, D.C.

So with respect to transparency, if there is a weakness, it's not because we are hiding things from you. It is -- I would suggest it is the changing nature of records.

And I see our department's records officer out there, so every chance I get to pitch Kathy Schultz and the "Federal Records Act," I do. And she's probably embarrassed now that I've referenced her. But that's okay because I always do whenever we're talking about records.

It's the changing nature of records and we've moved away from written hard copy memoranda on beautiful letterhead and mimeographed or carbon copy copies. And we now use electronic communications and e-mail. And so these things which really aren't ephemeral, especially if there is some congressional investigation or high profile litigation, we find out that they're not ephemeral.

But these electronic communications are not maintained the way they ought to be and so we don't keep the records like we ought to be keeping them. And that maybe makes it difficult for folks to know what we're doing, for historians down the road to understand why decisions were made within government.

And that's not something that's intentional. It's just we're catching up and our 55-, 56-year-old law, the "Federal Records Act," is now catching up to PDF and TIP and J Pegs and other electronic forms of communication.

MR. KROPF: Stephanie -- or Lina.

MS. ORNELAS: Well, transparency is a very difficult concept. It's slippery. And there are like at least a hundred definitions of transparency. But let's take only one.

If we think that transparency is seen through or looking through, I think as to personal data concerns, I think that the fact that we have now a system, at least in Mexico, that whereby you can see what kind of data the government is using and for what purposes.

You have like three steps. One is -- the first one is the notice and the privacy notice, you will receive it at the moment the government collects the data. And even we said before, you have to give this data. You cannot say the taxation authority I won't give you how much is my -- what's my income. You have to give it.

But at least you know that also this authority has your fingerprints. In Mexico, we have the electronic signature and you need to put your eight fingerprints. So you have to know what for this authority needs your fingerprints.

And if they storage this in a manner that has security measures, otherwise, a hacker can take this information out or if this authority sends information about or whatever -- so I think if you see through what the government is doing with your information, then you can react and you can access to your rights. Otherwise, what do you need a law and if you don't know it, if you don't have an authority that creates a culture that tells you that you have the right to know and the right to access and correct and et cetera. So I think it's

(unintelligible).

MR. KROPF: Thank you, Lina.

I think we're short on time here, but I'm going to open the floor up to concise and insightful questions and also turn to one of our panelists and give our panelist the option to ask a question.

I think, Stephanie, you had a question?

MS. PERRIN: Well, just a comment. I absolutely agree on the problem of the destruction of good old records systems for those of us who are gray haired here remember such things as file clerks and records rooms and, you know, decent filing systems.

Nevertheless, I give the Blackberry not just as an ad for Canadian technology, but –

(Laughter.)

MS. PERRIN: -- we used to talk and we had a decision from one of our more colorful provincial information commissioners, David Flaherty, who decided that backup tapes were not records under the control of the institution. This was many years ago and yours truly phoned him up and gave him my unabridged opinion of what I thought of that decision.

Nowadays we don't really talk about tapes. It's all going on to a hard drive. It would be even more difficult to make that argument that there are not documents under the control of the institution.

Furthermore, my argument that the time and now is if it's good enough for the Canadian police to come and arrest me under a warrant or not, it's a record.

So I think we're actually moving to more records and if these things are on a hard drive and searchable, it won't be as nice as the old paper files we had, but it will sure be searchable. So we need to sort of filter that into our thinking.

Now on with the legitimate questions.

MR. KROPF: Hugo.

MR. TEUFEL: We had some involvement with Blackberry recently. And fortunately that litigation was settled, but there were some concerns from a critical infrastructure standpoint.

And by the way, not all communications in Blackberry are retained on records if you're doing PIN to PIN.

MS. PERRIN: Right. We had the same problem and some people who ought to have known better didn't realize they weren't secure when they were going to PIN to PIN. So that ended that.

MR. KROPF: Fortunately I forgot my Blackberry today, so I'm not worried for today.

But turning to the audience, if you would just say your name and your affiliation.

MS. GREEN: I'm Lou Green. I'm in the Chief Counsel's Office at Customs and Border Protection.

And I guess I've been listening to sort of the processes of how one maintains information and how you're allowed to access it. But I think the one thing that I'm missing here is what happens when the government does release information that it's not supposed to and gets caught.

In the U.S., it's pretty clear for us you're subject, you know, criminal and civil penalties under U.S. law. But what of the other countries? What happens when you just do it and it's out there? What can a citizen do? What does the government do to the individual within that released the information?

MR. KROPF: Panelists?

MS. ORNELAS: Well, within the Mexican government, if they don't use personal data as the law says, so you are under administrative procedures under the -- on behalf of the comptroller, but also you can go to the tribunals and to the Judicial Branch to start the civil or a penal action. It depends on the harm.

If this information was related, for instance, with your business or -- while you can go to a specialized tribunal and everything. So we have a whole system working for that.

And till now we have a case in Mexico with the federal electoral authority and they

sold the database to Choice Point here in the states. And so all Mexicans older than 18 years including myself and the President are in those databases. We know that -- I mean, here it's not forbidden to share that information.

But the purpose of the federal authority in Mexico for -- it was electoral purposes for voting, for identifying yourself, not for your picture being in a lot of companies. I know that here you can also go and put your name on a no-call list and perhaps you won't be bothered by a company. But we don't know in Mexico, I mean, what can we do and if this information is all over the world, no?

So in Mexico, we created an institution to investigate this case. But till now there's no responsibility for this unfortunately. And our law was not enact when that case happened because the federal electoral authority is also subject of this law. But at that time, it wasn't.

So it's a bad case. But, anyway, there are like different actions you can act.

MR. JONES: The position in respect to individuals is fairly clear. So if an individual employee of the government department, just as an individual employee of the telephone company or bank, misused information they had access to, they used it for purposes that they shouldn't have done, they will commit a criminal offense for which they can be taken to court and prosecuted.

The other thing I would say is that for many years, particularly the UK police, have routinely prosecuted under data protection legislation. To be fair to them, they have been very, very clear to policemen about the privilege of access they have to highly detailed, sensitive records. And they've not only been -- I mean, obviously they sack them, but they quite often prosecute them as well.

It's the peculiarity of the UK law that the organization that misuses data doesn't actually commit a criminal offense. I mean, that's just the law they passed. It's a very strange law. So that the employee can commit an offense if they do that which they shouldn't have done. But if whatever the employer does, you know, they don't commit a criminal offense, they do leave themselves open to a compensation claim.

The other important point, I think, is I think that it is true that the UK government would be fairly -- is fairly sensitive about significant misdemeanors. Because we are not directly -- you know, we don't work to the government, our authority report directly to the House of Parliament. And what we can, therefore, do is put in our annual report to Parliament any failings that there are of the government.

So we can actually report that to Parliament. I'm not saying they quake terribly, but they're usually quite bothered about it. They'd prefer not to have that.

MS. PERRIN: I think that the situation is in flux in Canada with respect to this for a number of reasons.

Number one, as has been pointed out in the realm of identify theft that we do not actually have a way of bringing criminal charges against someone who is in possession of someone else's personal identity documents or fake ones that appear to purport to be those person's.

So the Department of Justice and the Department of Public Safety are supposed to bringing forward as the result of a consultation they did last -- I guess it's two years ago now legislated to fix this because if the police have been trying to go after identity theft and found niches with garbage bags full of stolen documents, they can report them to the privacy commissioner and we kind of gum them to death. We have no real authority to do anything at this point.

With respect to public servants breaching, not subject to disciplinary action. Presumably you could be fired. Ministers have been forced to resign over privacy breaches. So it's certainly enough no-no that people don't go running around in the federal government or the provincial government releasing data.

There is a "Whistle Blower Protection Act" that just came in that will permit this. The information commissioner didn't like it, various clauses in it. We'll see how it runs. And then we expect new things under this "Federal Accountability Act" that is coming in on the wings of quite a bit of abuse.

But there are provisions certainly for public servants to be criminally charged under breach of trust and abuse of authority if they release personal information. So we don't really need much.

The provisions that are in the private sector bill relate to destruction of data with a view to penalizing with criminal sanctions organizations that shred the data before the individual comes in to catch them red-handed with an access request.

DR. DIX: The situation in Germany is very similar to the one described for the UK and Canada. It is a criminal offense to not only disclose personal data illegally, but also to collect them illegally if you act with the intention to do harm or to actually for personal

profit, personal gain.

Otherwise, if these conditions are not fulfilled, it's still an administrative offense which may be -- for which you may be fined as a public servant.

To my experience, more of these cases have been brought in the public sector than in the private sector. I don't know exactly the reason for this, but this is -- and the examples of policemen, not that policemen are very prone or very often actually contravening the "Data Protection Act," but if they do so, they are being prosecuted quite consequently and disciplinary action is also being taken.

MR. KROPF: Thank you, panelists. We have one more question and then I think we have to wrap it up.

MR. WHITESNER: Thanks. Danny Weitzner, World Wide Web Consortium and MIT.

I wanted to come back to the question that Stephanie said was the hard question and Mr. Jones picked up on it. It was striking to me that it was on this panel, the international panel, that this question of de-identification and re-identification comes up. It's really what I think of as the question of data mining.

And as I spend a lot of time working on the World Wide Web, I'm aware more and more and I think we're all aware more and more of the power that the web has to expand our ability to use information.

I think the one thing we know about the web is that any one piece of information, personal or otherwise, really only can be -- has its meaning bounded by the web of information that it's part of that we never understand the scope or power of information, of a single atom of information, that that just doesn't exist particularly, at least in the world of the web anymore.

So I'm curious given the tremendous breadth of perspective here whether you have -- any of you have any sense of the direction that we might go in trying to address the problem that Stephanie identified that has been mentioned other times in the day, that the release of -- the import of the release of one piece of personal information or one piece of information, whether personal or not, which we can't always tell, simply can't -- doesn't seem to be well defined by that information.

And so how are we going to get our collective hands around this problem, do you

think? I'm not asking for the answer. I'm curious about what principles you think we could use. I thought the principle of public versus private purpose was interesting, but, frankly, seems like it would wear out very quickly. So I'm wondering where else you think we might go.

MS. PERRIN: Well, I can't answer my own question. And thank you for bringing it up again.

(Laughter.)

MS. PERRIN: But back in the early '90s when we were thinking about how to legislate in the private sector for privacy, I was in -- I think I was in international trade at the time. And we had a visit from the Swedish Justice Minister. And, of course, Sweden has lots of experience with very open records. And she said at the time that really we had to figure out how to attach purpose to each piece of data. And I thought that was quite far reaching at the time.

And we, in fact, put a clause in the PIPITA with respect to public information that hasn't actually had a lot of notice given to it, but it basically says you can only collect, use, and disclose publicly available information for the same purpose for which it was put on the public record.

So the intent was to try to corral people vacuuming up public records and using them for other purposes. I'm not suggesting for a minute it's going to be easy to police that, particularly when -- in Canada, you have charter right of creativity.

So if it's an individual gathering of this data through their searches, there's nothing you can do. Nevertheless, if it is a company gathering up this data, then you can indeed complain.

But I can't think of any better way to go after this than to make it an offense to have data that you don't have the authority, a legitimate purpose that will pass a reasonable person test to have in your possession. Otherwise, we might as well just give up and all go home.

I am struck -- when I was a "FOIA" officer in Canada, we do have oversight over the intelligence agencies, CSE and all of these people. And they would come in very solemnly when we had an access request and say you can't release that nondescript piece of information because of the mosaic effect. And you heard that argument down here, of course. I'm sure we stole the term from you.

It's exactly that mosaic effect that is killing us now in the personal data re-identification and we have to do something about it. So what's sauce for the goose is sauce for the gander as far as I'm concerned.

MR. KROPF: Alexander.

DR. DIX: I think in the long run, we need to reconsider the concept of personal data and maybe that is what Stephanie has already meant. We will probably have to address the questions of group discrimination, information or discrimination of groups.

In Germany, we have now a discussion about people being -- receiving negative credit ratings because they are living in certain neighborhoods, people being put back into the queue when you call a call center. You wonder why it takes so long someone's answering your call. It's because you're calling from the wrong zip code.

So these are the questions, entirely new questions going way beyond conventional personal data protection. So that we have to think about.

MR. KROPF: Phil, I think you had –

MR. JONES: Just very briefly. I mean, there's no magic answers, I mean, like Stephanie wants.

One of the things we try to do in the UK, and this only covers public information, publicly available stuff, for a long time effectively citizens were required to register to vote or risk committing a criminal offense. And then the electoral registration officer was required to sell that list to anybody who wanted to buy it to use how they wanted.

Deleted: (unintelligible)

Now, we objected for a long time and nobody says anything. But then these rolls started appearing on web sites and then you had people who worked in the agriculture department or other people in sensitive jobs who kicked up a fuss.

And now we do actually have some control over any secondary use that's made of the electoral roll. I think what we think is there's a real need for government -- we said this to them -- to revisit all their public registers and look at the amount of information that's there, home addresses, et cetera.

So the whole need to revisit all that in the light of the tremendously changed privacy risk there is that the new technologies have brought with them because you used

to be able to get hold of land records, but you used to have to go there, go to this dusty filing cabinet, spend hours going through. That doesn't happen anymore. You sit at the desk and press two buttons. So I think there is a big issue there.

The other issue that you raise, I think, is harder. The bit about where you release information that genuinely to your best efforts you think is likely to be de-identified or reasonably anatomized, how much computing power you assume it -- because the way parameters -- you know, parameters change, things move on quickly. You don't always spot everything.

And, of course, the tension is that if you become too cautious, there are whole areas where you don't release aggregate information whether a really good public policy or academic reasons for doing it. For that reason, I think it's really difficult because I don't think there's an easy answer.

MR. KROPF: I think Phil is going to have the last word seeing as we have run over. I would like to thank the panelists for their insights. I would like to thank the audience for your patience.

And I would like to turn the floor over to Maureen Cooney.

(Applause.)