**25TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS**
**SYDNEY, AUSTRALIA, 12 SEPTEMBER 2003**

# MINUTES OF THE CLOSED SESSION HELD ON 12TH SEPTEMBER 2003

## 1. Welcome and Agenda

Mr Malcolm Crompton, as Host of the 2003 Conference and Chair, welcomed delegates to the Closed Session of the 25th International Conference on behalf of the co-hosts the Privacy Commissioners of New South Wales and Victoria. With the agreement of the other participates, he announced a change to the previously adopted agenda. Ms Nuala O'Connor Kelly, Chief Privacy Officer, US Department of Homeland Security would be present for fifteen to twenty minutes at the commencement of the meeting to answer questions from Commissioners.

## 2. Question and Answer Session with Nuala O'Connor Kelly

Ms Nuala O'Connor Kelly was invited into the session at this point. Discussion took place with Ms O'Connor Kelly that clarified the degree of independence her Office has including the ability to report to Congress without direction. The size of the Office of the Chief Privacy Officer and Department of Homeland Security and other matters were also discussed.

The meeting expressed its appreciation to Ms O'Connor Kelly for her candid discussion of the circumstances of her Office with Commissioners in the Closed Session.

## 3. Report of the Credentials Committee and Resolution on Accreditation

On behalf of the Credentials Committee Mr Bruce Slane, Commissioner, Office of the Privacy Commissioner, New Zealand introduced the written report. Please refer to Attachment A for the content of this report.

Mr Slane informed the meeting that this year 11 applications had to be considered against the criteria established at the 23rd Conference in Paris. Mr Slane explained that each application is assessed against the accreditation principles and a recommendation is made about each applicant. Mr Slane advised meeting participants that this year's report outlined the processes that the Committee established for undertaking the Committee's work.

Of the 11 applications received, 3 were at the national level, 3 at the sub national level, and 5 at supranational level. All were recommended for accreditation.

The 5 applications from organisations at the supranational level were given special consideration by the Committee to recommend whether they should receive a vote. Mr Slane explained that given the narrow scope of the 5 international applications the Committee did not feel the need to grant voting rights.

The Committee agreed to serve another term since the rules permit re-election. Mr Slane's successor will represent the Office of the Privacy Commissioner, New Zealand on the Credentials Committee.

Italy put forward the suggestion that the issue of supranational organisations be discussed at the European Commissioners meeting in November.

The Resolution on Accreditation was adopted with consensus and without further amendments. This Resolution is at Attachment B.

## 4. Matters arising from the 24th International Conference

Mr Joe Meade, Data Protection Commissioner, Ireland gave a brief report noting that the success of the 24th Conference was due to the secretariat backup provided from the UK Office. Mr Meade indicated that the Conference generated media interest that followed on from 11 September 2001. There were no other matters arising from the 24th International Conference.

## 5. Formal Resolutions

For the formal resolutions the role of Chair was undertaken by Mr Paul Chadwick, Privacy Commissioner of Victoria, Australia.

### 5.1. Resolution on improving the communication of data protection and privacy information practices [Australia]

This Resolution proposed by Australia was also the subject of a workshop held during the open Conference the previous day. 6 Authorities cosponsored the Resolution: Commissioner for Data Protection and Access to Information, Brandenburg, Germany; Commission Nationale de l'Informatique et des Libertés (CNIL), France; Data Protection Commissioner, Czech Republic; Hellenic Data Protection Authority; Independent Centre for Privacy Protection, Schleswig-Holstein; State Data Protection Inspectorate, Republic of Lithuania and the Dutch Data Protection Authority.

The UK Information Commissioner, Mr Richard Thomas briefly commented that although the UK office was not formally listed as cosponsors the UK Office did take part in the email correspondence and supported the Resolution as well.

The Resolution was adopted without amendment. The resolution as adopted is at Attachment C.

### 5.2. Resolution on Automatic Software Updates [Germany]

This Resolution was put forward by the Commissioner for Data Protection and Access to Information, Brandenburg, Dr Alexander Dix and was circulated among the delegates in a new English-only version. Italy expressed its full support and was included as a co-sponsor along with the other cosponsors: the Data Protection Commissioners of Germany; the Czech Republic; the State Data Protection Inspectorate of the Republic of Lithuania; the Information and Privacy Commissioner of Ontario and the Swiss Federal Data Protection Commissioner.

The newly amended Resolution (Italy as co-sponsor) was adopted with consensus and without further amendments. The Resolution as adopted is at Attachment D.

### 5.3. Resolution on International Agencies [New Zealand]

This Resolution put forward by the Office of the Privacy Commissioner, New Zealand was introduced by a PowerPoint Presentation delivered by the Assistant Privacy Commissioner of New Zealand, Mr Blair Stewart. In the final part of his presentation Mr Stewart recommended that the host of the 25th Conference write to those bodies to elicit a response and start a dialogue. Mr Stewart noted that this could create work for the host and proposed that cosponsors to the resolution assist with the task and called for other suggestions to be submitted to the host of the Conference. Mr Stewart suggested that the group report back about whether the resolution had elicited any change at the next Conference.

The President of the CNIL, M Michel Gentot, commented that the final part of Mr Stewart's presentation imposes a heavy responsibility on Australia to broadcast the resolution. M Gentot suggested that all the bodies present should transmit to those organisations that should be notified, the details of the Resolution.

Mr Crompton responded by indicating that any help the Australian Office could receive in discharging the resolution would be gratefully received. Mr Crompton pointed out that the scale of the task was unknown and that there were probably untold hundreds of supranational bodies who may fit the description. The sponsor and cosponsors agreed that they would prepare the list of organisations who they considered should receive the letter (including all contact details) and would prepare a draft covering letter.

Please find the Resolution as adopted at Attachment E.

### 5.4. Resolution on Passengers' Data Transfer [Switzerland]

The Resolution put forward and introduced by the Swiss Federal Data Protection Commissioner, M Jean-Philippe Walter. The Spanish delegation suggested that the 3rd dot point at Item A be altered to reflect other transport providers and not just airlines. There was acceptance from the meeting for this suggestion. Mr Chadwick also noted for drafting purposes that the word "airlines" should also be removed from the resolution so that reservations applied to any transport providers, and that the final sentence should be amended to reflect "those providers" rather than the word "airlines".

The newly amended Resolution was adopted by consensus. The Resolution as adopted is at Attachment F.

### 5.5. Draft Resolution on RFIDs [Germany]

Mr Crompton resumed as Chair and called upon the Commissioner for Data Protection and Access to Information, Brandenburg, Dr Alexander Dix to address the meeting with regard to his draft resolution on RFIDs. Dr Dix advised the meeting that a proposal on radio frequency identification was circulated prior to the Conference however this was outside the two week deadline required to

submit resolutions for consideration at the closed session and therefore could not be considered at this meeting.

It was agreed that Dr Dix would circulate a document after the Conference and that the meeting would come to a consensus on the issues of RFID technology soon after the Conference by e-mail.

[Mr Crompton circulated the resolution, as finalised by Commissioners, on 3 December. The Resolution is at Attachment G.]

## 6. Report on the International Working Group on Data Protection in Telecommunications (IWGDPT) by Hansjürgen Garstka

The report on the work of the IWGDPT was presented by the convenor, Hansjürgen Garstka, Data Protection & Information Access Commissioner of the State of Berlin.

Mr Garstka informed the meeting that since the last international conference the Group had met on three occasions. It was the twentieth year in which the Group had met since 1983 when it was founded in connection with the Radio Symposium.

The Group had two working papers on intrusion detection systems over data protection processes getting into computers and looking how people get into computers. The Group also has a working group on the adoption of ENUM services.

Mr Garstka indicated that an item that always appears on the agenda is the issue of cyber crime and in particular, data retention regulations. Mr Garstka also advised that the Group has dealt with a lot of people in relation to domain names and have also been in contact with the system that regulates domain names on the internet.

Mr Garstka outlined the matters currently being addressed by the Group included:

- Regional availability of a document on the Internet instead of the current global availability
- SPAM
- Media privilege and privacy
- MMS
- Privacy friendly protection against deception on the internet and
- smart updates and radio frequency ID

Mr Garstka advised that the next meeting will take place in Buenos Aries in Argentina. Although not yet confirmed the meeting is planned to take place 7 April 2004.

## 7. Speech by Mr Paul Thomas on "Safety requirements: A task for Data Protection Commissioners?"

Mr Paul Thomas President of the Belgian Data Protection Commission addressed the meeting on the above subject. Mr Thomas' paper is available at Attachment H.

## 8. Future Conferences

Mr Crompton acknowledged the unfortunate incident and series of developments in Canada over the last year, which have meant that Canada was not in a position to host the Conference in 2004.

Dr Dix advised that the Inspector General for the Protection of Personal Data, Poland had asked him to convey her cordial invitation to hold the 2004 Conference in Poland. The meeting agreed to this proposal and thanked Poland warmly for assisting in this way at such a late time. The venue and the date have not yet been fixed, however there is clear indication that the meeting would certainly not take place in Warsaw.

Switzerland was confirmed as convenor in 2005.

The meeting noted the interest in Argentina holding a conference at some point in the future.

## 9. Question & Answer Session on Country Reports

Copies of country reports were circulated prior to and distributed at the Conference. There was no further discussion of these reports at the meeting.

## 10. Closing remarks

Mr Crompton took the opportunity to pay tribute to retiring Commissioners, notably Bruce Slane, Michael Smith, Joachim Jacob and Paul Thomas and praised them for their contributions. The meeting recorded a general vote of thanks to these colleagues.

Mr Bruce Slane acknowledged the kind remarks and noted that the meeting should formally record its appreciation to the Office of the Federal Privacy Commissioner, Australia, to the Commissioner and Deputy Commissioner, and all the staff who have been involved in organising the Conference. Mr Crompton accepted the thanks on behalf of everybody in the Office, and the colleagues in NSW and Victoria.

Mr Crompton drew the meeting to a close outlining the challenge of facilitating communication between all commissioners between conferences. He requested that when the resolution which Dr Dix will circulate on RFID tags is received, the group advise each other of any errors or changes in email address. This would then form the basis for the next host's communication with Commissioners.

**Attachment A**

**25TH INTERNATIONAL CONFERENCE OF DATA PROTECTION AND PRIVACY COMMISSIONERS**
**SYDNEY, AUSTRALIA, 12 SEPTEMBER 2003**

## *Report of the Credentials Committee*

The Credentials Committee comprising the commissioners from France, New Zealand and the United Kingdom was elected at the 23rd Conference for a 2-year term. At the 24th conference it was noted that the UK Commissioner would leave her post prior to the 25th conference. It was the wish of the conference that her successor should take her place to maintain continuity with the work already undertaken. Accordingly, this year the Credentials Committee comprised:

- Michel Gentot, President of CNIL, France
- Bruce Slane, Privacy Commissioner, New Zealand
- Richard Thomas, Information Commissioner, United Kingdom.

To assist it in its work, the Committee continued the arrangement for a senior staff member from each office to form a subgroup. The Credentials sub-group comprised:

- Marie Georges, Head of European and International Affairs Division, CNIL, France
- Blair Stewart, Assistant Privacy Commissioner, New Zealand
- Jonathan Bamford, Assistant Information Commissioner, United Kingdom.

The Credentials Committee, and the sub-group, maintained a continuity not only with last year's work but stretching back to the working group set up by the 22nd Conference to recommend suitable accreditation criteria.

### The task

The Committee's role derives from the "Resolution on Accreditation Features of Data Protection Authorities" adopted at the 23rd conference. The Committee's task is to process applications from any authority that wishes to be accredited to participate in the conference. The Committee assesses each application against the accreditation principles and recommends to the conference the authorities that ought to be accredited and in what category. The committee's recommendations, in the form of a resolution, are the first item of conference business at the closed session.

Last year's report outlined the processes that the committee established for undertaking its work. Those processes worked successfully during the major exercise prior to the 24th conference of accrediting most existing data protection authorities. They were utilised again this year.

### National and sub-national level applications

This year 11 applications were received, 3 at national and 3 at sub-national level.

The committee is pleased to draw the conference's attention to:

- the first authority from South America – Argentina
- the first authority to combine privacy, freedom of information and archives within its remit – the Northern Territory of Australia.

The applications from Alberta, which has been represented at the conference previously, and from the newly created authorities in Cyprus, Malta and the region of Madrid, are also acknowledged. All have been recommended for accreditation.

**International and supra-national level applications**

For the first time the committee received applications from authorities within supra-national or international bodies. Much of the sub-group's time was spent on studying these applications and exploring with the Committee the way in which the particular issues should be approached.

The Committee received 5 applications from authorities within the following international or supra-national bodies:

- Council of Europe
- Interpol
- European Union (Europol, Schengen Information System, Customs Information System).

The Committee has two tasks. The first, as with all applicants, is to assess the authority to see whether it meets the requirements of the accreditation principles. The second is specific to the authorities at the international or supra-national level. That is to consider whether to recommend that the authority in question exercise a vote at the conference (refer clause 2, Addendum to Guidelines and Procedures for Conference Resolutions).

The Committee was satisfied, on balance, that each of the applicants should be recommended for accreditation. As noted last year, the Committee had developed a methodology to assess each application using a standard checklist focusing upon whether:

- the authority has clear and wide ranging data protection functions covering a broad area of economic activity
- the authority is a public body established on an appropriate legal basis
- the authority is guaranteed an appropriate degree of autonomy and independence to perform its functions
- the law under which it operates is compatible with international instruments
- the authority has an appropriate range of functions with the legal powers necessary to perform those functions.

On the first point, the authorities each had a relatively narrow sphere of competence which gave the Committee pause for thought. Had an application been received from a national or sub-national authority with jurisdiction solely over a particular law enforcement database the Committee would not have recommended accreditation for such a narrow specialist entity. Even the authority in relation to the Council of Europe has reasonably narrow competence. However, given the importance of institutional data protection at this level, the otherwise satisfactory nature of the applications and the fact that an international or supra-national authority will never be exactly like a national counterpart, the Committee is minded to support accreditation in each case. Given the

narrow spheres of competence, the Committee does not recommend granting voting rights in any case.

A further consideration bearing upon voting rights is that three of the applicants have competence in relation to EU institutions or systems. Were voting rights to be granted to each, there would be an inconsistency with the approach taken in relation to the national and sub-national level authorities, namely that one international body would have more votes than any individual country. The EU issue may become clearer when the position of EU Data Protection Supervisor is filled. That authority will have a broader range of competence which may merit the granting of a vote. However, that is a question for a future committee and conference.

**Other matters**

The minutes of the Cardiff conference note that the Committee was asked to consider again the approach taken to Jersey, Guernsey and the Isle of Man. The Committee reaffirms its earlier recommendation that these authorities remain accredited at sub-national level.

Michel Gentot
Bruce Slane
Richard Thomas
**Credentials Committee**

**Attachment B**

**ACCREDITATION RESOLUTION**

The Credentials Committee proposes the following resolution in relation to **accreditation of authorities** to participate in the international conference:

That the International Conference accredits the authorities listed in the Schedule.

Michel Gentot
Richard Thomas
Bruce Slane

**Credentials Committee**

## SCHEDULE

### A NATIONAL AUTHORITIES

**Argentina**: National Direction for Personal Data Protection (Director Nacional de Protección de Datos Personales)

**Cyprus**: Personal Data Protection Commissioner

**Malta**: Data Protection Commissioner

### B AUTHORITIES WITH A LIMITED SUB-NATIONAL TERRITORY

**Australia**

- Northern Territory: Information Commissioner

**Canada**:

- Alberta: Information and Privacy Commissioner

**Spain**

- Madrid: Data Protection Agency of the Region of Madrid (Agencia de Protección de Datos de la Comunidad de Madrid)

### C AUTHORITIES WITHIN AN INTERNATIONAL SUPRA-NATIONAL BODY

**Council of Europe**: Data Protection Commissioner

**European Union**:

- Customs Information System Joint Supervisory Authority

- Joint Supervisory Body of Europol
- Joint Supervisory Authority for Schengen Information System

**Interpol**: Commission for the Control of Interpol's Files (Commission de Contrôle des Fichiers de l'O.I.P.C.-Interpol)

---

## Explanatory Note

In accordance with rule 4 of the Rules for the Credentials Committee, and clause 1 of the Addendum to the Guidelines and Procedures of the Conference Resolutions, this resolution sets out recommendations for accreditation for authorities to participate in the international conference under appropriate classification. The resolution and the names of the countries, territories, authorities and international supra-national bodies are given in English. Where an authority has a title in a language other than English this is given in brackets (where known).

Authorities within an international or supra-national body which have been duly accredited may attend and participate in meetings but will not be entitled to vote unless the Conference has specially decided to grant them voting rights at the time of accreditation (see Addendum to the Guidelines and Procedures for Conference Resolutions, clause 2). The Committee does not recommend that voting rights be conferred upon any of the 5 authorities within international or supranational bodies affected by this resolution

**Attachment C**

**25TH INTERNATIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS**
**SYDNEY, 12 SEPTEMBER 2003**

Resolution on improving the communication of data protection and privacy information practices

**Proposer:** Privacy Commissioner, Australia

**Co-sponsors:**

- Commissioner for Data Protection and Access to Information, Brandenberg, Germany**;**
- Commission Nationale de l'Informatique et des Libertés, France
- Data Protection Commissioner, Czech Republic;
- Hellenic Data Protection Authority,
- Independent Centre for Privacy Protection, Schleswig-Holstein,
- State Data Protection Inspectorate, Republic of Lithuania,
- Dutch Data Protection Authority.

**Resolution**

That the 25th International Conference of Privacy and Data Protection Commissioners resolves that:

1 The conference calls the attention of organisations, in both public and private sectors, to the importance of:

- improving significantly their communication of information on how they handle and process personal information;
- achieving global consistency in the way they communicate this information;

and by these means

- improving individuals' understanding and awareness of their rights and choices and their ability to act on them; and
- putting an incentive on organisations to improve, and make more fair, their information handling and processing practices as a consequence of this awareness.

2 The conference endorses the following means of achieving these goals:

- development and use of a condensed format for presenting an overview of privacy information that is standardised world wide across all organisations which sets out:
    - the information that is most important for individuals to know; and
      the information that individuals are most likely to want to know; and
      the use of simple, unambiguous and direct language;
    - the use of the language of the website or form which is used to collect information;

- confining the format to a limited number of elements which, consistent with the above, covers important data protection principles like:
    - who is collecting the personal information and how to contact it (at least the official name of the organisation and physical address);
    - what personal information the organisation collects and by what means;
      the purposes for which the organisation is collecting the personal information;
    - whether the personal information is to be disclosed to other organisations and, if so, the kinds or names of organisations and for what purposes;
    - the privacy choices the individuals have and how to exercise them easily, in particular, choices about whether personal information can be disclosed to third parties for unrelated but lawful purposes and about which personal information individuals must provide to receive a service;
    - a summary of the individual's rights of access, correction, blocking or deletion;
    - the independent supervisory body to which individuals may complain if they are concerned that their rights have been breached.
- the use of appropriate means to enable individuals to find further information easily including:
    - information that any applicable law requires an organisation to provide, including rights of access, correction, blocking or deletion, and how long an organisation retains personal information; and
    - a complete explanation of the information summarised in the condensed format; and
    - the complete statement of an organisation's information handling and processing practices.

3 The conference agrees that such standardised and condensed format should be consistent with all national laws that may apply, and is to be in addition to, where necessary, and consistent with, any notices that an organisation is legally required to give an individual.

4 The conference is aware of the importance of the timing of presentation of data protection and privacy information to the individual. For example, it is particularly desirable for information to be presented automatically at the point where individuals have the chance to choose what information they give, and whether information can be disclosed to third parties. In other cases it may be appropriate to leave individuals to seek data protection and privacy information via obvious links. The conference is aware of the important work the EU Article 29 Data Protection Working Party has done on the automatic presentation of data protection and privacy information in *Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union.*

5 The conference considers the timing for the presentation of the condensed format (which takes into account both the on and off-line environments) would be a fruitful area of further work for Data Protection and Privacy Commissioners.

6 The Conference is also aware of related activities such as the development of computer languages describing privacy policies. It encourages the further development of ways to translate those policies into the standardised and condensed format.

7 The conference sees these as first steps to encourage better practice in the way organisations communicate privacy information about how they handle or process personal information. The conference is aware of initiatives in this area and encourages any such initiatives to improve communication between organisations and individuals. The Conference looks forward to working with organisations and interest groups that are taking such steps and it expects to take further steps to improve on communications between organisations and individuals in future conferences.

**Explanatory notes**

This resolution aims to reach agreement about the need for public and private sector organisations to better communicate information about the way they handle and process personal information.

**Why this resolution is important**

A significant number of countries around the world have privacy law, or other laws, that require companies and other organisations collecting personal information to give consumers information about their privacy practices. Ensuring people are well informed about what an organisation does with their personal information is one of the main ways that laws seek to protect privacy. This enables people to exercise choice and have control over their personal information.

This resolution is important because there is growing evidence, however, that despite the volumes of documents and information that organisations are providing, individuals are not well informed about the privacy practices of the organisations they deal with, (see for example, a recent report from the Annenberg Public Policy Center of the University of Pennsylvania, *Americans and Online Privacy: The system is Broken* http://www.asc.upenn.edu/usr/jturow/internet-privacy-report/new.html) and that further work is needed to ensure that individuals get the information they need at the right time to place their trust in the sites with which they are interacting. (See for example, the *Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union* http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2001/wpdocs01_en.htm). The Annenberg Public Policy Center research also provides evidence confirming that individuals will spend very little time and effort to find out about such information.

A further challenge is to enable individuals to be well informed and able to exercise choices when the organisations with which they are dealing operate globally. For example, Action 6, "More harmonised information provisions" in the recent European Commission *Report on the transposition of Directive 95/46/EC* calls for a more harmonised approach to providing notice to individuals (http://europa.eu.int/comm/internal_market/privacy/lawreport/data-directive_en.htm).

**What the resolution is trying to achieve**

There is now considerable research on how organisations can improve communication with individuals when individuals need to be given important information. Much of this has happened in the area of food labelling. (See for example, James R. Bettman, John Payne and Richard Staelin, 'Cognitive Considerations in Effective Labels for Presenting Risk Information', *Journal of Public Policy & Marketing*, Vol 5, 1986, p.1-28.). However, there has also been quite a bit or work done in relation to better communicating information about an organisation's personal information handling practices. Simplification of notification procedures is on the 2003 work program for the European Union Article 29 Data Protection Working Party.

(http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2003/wpdocs03_en.htm). Work has also been done on improving notice in the US (http://www.ftc.gov/bcp/workshops/glb/index.html) and by the P3P user agent taskforce (http://www.w3.org/P3P/2003/p3p-translation.htm).

The result of this work shows that an important first step to improving communication in both the on and offline environment is;

- a shorter format for providing information, with a limited number of elements (some research says 6 or 7);
- including just the basic information that individuals want to and need to know;
- standardisation to develop familiarity, education and ability to compare;
- simpler, non-legalistic language, and use of everyday terminology;
- clear and easy access to further information.

This resolution focuses on these matters as being an important first step in improving communication. There are, however, a number of other very important dimensions to achieving this, which it not possible for this resolution to cover in detail.

The next important step is presenting information about an organisation's information handling practices at the right time. Again, the EU Article 29 Data Protection Working Party has done a considerable amount of work on this particularly in the online environment in *Recommendation 2/2001 on certain minimum requirements for collecting personal data on-line in the European Union* (http://europa.eu.int/comm/internal_market/privacy/workingroup/wp2001/wpdocs01_en.htm). Ensuring that the right information is presented at the right time is a complex area. The right time may vary depending on the medium the person is using to interact with an organisation. For this reason, the resolution proposes that this could be a fruitful area of future work for data protection and privacy commissioners.

Although the individual would be the main beneficiary of improved communication of information about an organisation's privacy practices, there are also likely to be benefits for business. For example, organisations could achieve better relationships with their clients in the form of trust and loyalty. A standardised format that could be used by a company globally could provide economies of scale.

**The drafting process**

Having identified the problem of inadequate communication of information about an organisation's personal information handling practices as being a possibly global issue, the Office of the Federal Privacy Commissioner, Australia, asked accredited data protection and privacy commissioners by email if they agreed that this was an important issue and an appropriate topic for a resolution at the 25th International Conference of Data Protection and Privacy Commissioners (http://www.privacyconference2003.org/). The Office then sent another email outlining the issue further. Eighteen out of the twenty-seven Commissioners who responded to these emails agreed that this was an important issue. On the basis of these responses the Office invited Commissioners from Brandenburg, Czech Republic, France, Greece, Hong Kong, Italy, Lithuania, Netherlands, Poland and the United Kingdom to form a working group to work on the draft of the resolution which is now circulated with this explanatory note.

Before the conference, the Office of the Privacy Commissioner, Australia created a webpage with background material on it. This material aims to help understanding of the debate about improving communication of information about privacy practices. This is available at http://www.privacyconference2003.org/resolution.asp.

The issues behind the resolution will also be discussed in a workshop session open to all registered participants in the 25th International Conference of Data Protection Commissioners, before Commissioners formally consider the resolution.

**Points about content of the resolution**

The resolution assumes that organisations will comply with their notification requirements under the law. The standardised condensed format proposed in the resolution would (unless an organisation does not need to provide any more information) be in addition to these requirements.

Some people may be concerned that organisations should also be improving their information handling practices, or that the privacy laws applying to organisations should be strengthened. These are very big issues that cannot easily be dealt with in one resolution. Instead, this resolution is taking one first and small, but achievable, step of seeking to achieve effective communication of information about the current handling practices of organisations. It deals with this communication issue as separate from the much more complex one of whether, for whatever reason, those practices need improving. Of course, the practices an organisation communicates about must be consistent with any applicable law.

The purpose of providing a condensed format is to greatly improve the chances that individuals will at least read and understand the most important privacy information. This would be an important practical improvement on the current situation which appears to be that many individuals do not read or understand very much of the information that organisations provide. The resolution therefore picks out the elements of information about an organisation's information handling practices identified by the working group as being the most important to be included, based on research to date and its own knowledge. There are, of course other important elements. However including them in the condensed format would make it too long and would defeat the purpose of the resolution which is to achieve effective communication. The resolution deals with this dilemma by urging organisations to provide appropriate means to enable individuals to find further information easily, including the all the rest of the information that the law may require an organisation to provide.

If a condensed format is to be standardised globally and across organisations, there are limits on the kind of information that can be included in the format. For example, laws about rights of access vary from country to country. Trying to set out all the possible applicable rights an individual might have globally in a condensed format would make it too long. The resolution approaches this problem by providing that the format should summarise access rights and then provide the means for individuals to find further information.

It is very important that the information an organisation includes in a condensed format does not mislead individuals about the organisation's practices. For this reason, the resolution provides that the condensed format must be consistent with all national laws that apply, and this would include any laws prohibiting organisations from engaging in misleading and deceptive conduct. If organisations take sufficient care, information in the condensed format can be framed so that individuals can get an accurate snapshot of an organisation's practices. The resolution also

addresses this issue by requiring the format to include information about the independent supervisory body to which individuals may complain if they are concerned that their rights have been breached

Finally, the working group seeks to ensure that the work begun by passing this resolution does not end there. The final paragraph of the resolution therefore suggests that the way forward is for Commissioners to work with all those working on improving communication in the way suggested by the resolution to ensure that the next necessary steps are taken.

**Attachment D**

**25TH INTERNATIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS**
**SYDNEY, 12 SEPTEMBER 2003**

Resolution on Automatic Software Updates

**Resolution**

The Data Protection Commissioners of Germany, the Czech Republic, Italy, the State Data Protection Inspectorate of the Republic of Lithuania, the Information and Privacy Commissioner of Ontario and the Swiss Federal Data Protection Commissioner propose that the International Conference resolve that:

1. The Conference notes with concern that software manufacturers worldwide increasingly use non-transparent techniques to transfer software updates to users' computers. In doing so they
   - can read and collect personal information stored on the user's computer (e.g. browser settings, and information on the user's browsing habits) without the user being able to notice, to influence or to prevent it,
   - may gain at least partial control over the target computer thereby restricting the ability of the user to meet his legal obligations and responsibilities as a controller to ensure the security of any personal data he may be processing,
   - change the software installed on the computer which will then be used without any required testing or clearance and
   - may bring about malfunctions in the updated computer without the possibility to identify the update as the cause.

   This may cause particular problems in government institutions and private companies to the extent that they are under specific legal obligations how to process personal information.

2. The Conference therefore calls on software companies
   a. to offer procedures to update software online only at the user's initiative or request, in a transparent way and without allowing unchecked access to the user's computer;
   b. to ask for the disclosure of personal data only with the informed consent of the user and insofar as it is necessary to carry out the online update. Users should not be forced to identify (as opposed to authenticate) themselves before they can initiate the download process;
   c. to provide for freedom of choice by offering online updates only as an alternative to other (offline) means of software distribution such as CD-ROM.

3. The conference encourages the development and implementation of techniques to update software which respect the privacy and autonomy of computer users.

**Attachment E**

**25TH INTERNATIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS**
**SYDNEY, 12 SEPTEMBER 2003**

Resolution on Data Protection and International Organisations

**Proposer:** Privacy Commissioner, New Zealand

**Co-sponsors:**

- Data Protection Commissioner, Ireland
- Commission Nationale de l'Informatique et des Libertés, France
- Privacy Commissioner for Personal Data, Hong Kong SAR
- Federal Data Protection Commissioner, Germany

**Resolution**

That the 25th International Conference of Privacy and Data Protection Commissioners resolve:

That the conference calls upon:

(a) international and supra-national bodies to formally commit themselves to abiding by principles that are compatible with the principal international instruments dealing with data protection and privacy;

(b) international and supra-national bodies that hold or process personal data to establish appropriate mechanisms to ensure compliance with applicable data protection principles, such as the establishment of internal but operationally independent supervisory authorities with control powers;

(c) international and supra-national bodies that have a role in promulgating standards, rules or common practices which affect personal data handling within the jurisdictions of their constituent members to develop and adopt suitable mechanisms to ensure that data protection considerations are effectively taken into account, such as the use of privacy impact assessments and consultation with recognised data protection authorities;

and requests the host of the 25th International Conference to draw this resolution to the attention of the relevant bodies.

**Explanatory note**

The International Conference, now in its 25th year, primarily consists of national data protection and, in federal and devolved jurisdictions, their sub-national counterparts. Building upon preliminary work at the 21st and 22nd conferences, the 23rd conference resolved to establish a process and criteria for recognising the credentials of data protection authorities. The Paris resolution explicitly anticipated data protection authorities within international and supra-national bodies. The conference will, this year, be called upon to consider for the first time the accreditation of authorities at international and supra-national level.

There are data protection rules applying to some key institutions, arrangements and databases at the international or supra-national level but many new information sharing arrangements are being

initiated through a variety of international bodies. Not all of these bodies have previously had much exposure to data protection approaches and the issues are often being considered, if at all, very late in international standard setting processes.

Many law enforcement initiatives come to mind in this context. However, also consider, for example, the following current examples of initiatives from specialist bodies having having widespread effects:

- significant initiatives to add biometrics to passports will flow from standard setting by the International Civil Aviation Organisation (see www.icao.int )
- a sports drug testing code and associated standards recently issued by the World Anti-Doping Agency, includes new obligations regarding the sharing of information about individual athletes' whereabouts (see www.wada-ama.org )
- the ENUM proposals to combine telephone numbers and email addresses arise from a working group of the Internet Engineering Task Force and International Telecommunications Union (see www.enum-forum.org).

Even international organisations which have been involved in data protection in one capacity may lose their awareness if they lack an institutional check on their practices. For example, the "privacy notice" on the United Nations website does not mention the UN's own Guidelines concerning Computerised Data Files (1990) adopted by the General Assembly.

Appropriate data protection of information held by international and supra-national organisations cannot be achieved solely by national laws and data protection commissioners. International organisations need themselves to adopt appropriate standards, policies and principles and to establish mechanisms to ensure that they are carried into effect. This resolution encourages such steps to be taken in a manner which accords with internationally recognised practice. Furthermore, international bodies are responsible for promulgating both "hard law" and, increasingly, "soft law" at international level which must then be carried forward at national level. While such international standard setting is often to be welcomed, it can cause particular difficulties at national level if the data protection dimension has not been considered within the international standard setting. By adopting this resolution, it is hoped to encourage better awareness and compliance within international institutions which may, almost as a by-product, better inform those bodies when undertaking international standard setting (including setting up effective mechanisms to consult existing data protection authorities on matters affecting their jurisdictions).

The Conference host is requested to draw the attention of relevant international bodies to the resolution. He may wish to consult with the sponsors of the resolution in relation to that task. It is anticipated that a short report on the outcome of that process would be submitted to the 26th conference.

**Attachment F**

**25TH INTERNATIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS**
**SYDNEY, 12 SEPTEMBER 2003**

Resolution concerning the Transfer of Passengers' Data

The 25th International Conference of Privacy and Data Protection Commissioners resolves:

A. The Conference notes that

1. In the course of the legitimate struggle against terrorism and organized crime measures are being considered in some countries that could threaten fundamental rights and freedoms, in particular the right to privacy.
2. There is a danger of undermining democracy and freedom by measures designed to defend it.
3. Legal requirements on airlines and other transport providers to provide access to, or transfer data from, comprehensive passenger data stored in reservation systems could conflict with international data protection principles or those providers' obligations under national data protection laws.

B. The Conference therefore affirms that

1. In the fight against terrorism and organized crime, countries should determine their responses paying full regard to fundamental data protection principles, which are integral parts of the values being defended.
2. Where regular international transfers of personal data are necessary, they should take place within a framework taking data protection into account, e.g. on the basis of an international agreement stipulating adequate data protection requirements, including clear purpose limitation, adequate and non-excessive data collection, limited data retention time, information provision to data subjects, the assurance of data subject rights and independent supervision.

**Attachment G**

**25TH INTERNATIONAL CONFERENCE OF DATA PROTECTION &**
**Privacy Commissioners**
**Sydney, 12 September 2003**

Resolution on Radio-Frequency Identification

Final Version
20 November 2003

Following a proposal by the Data Protection and Access to Information Commissioner Brandenburg, the Independent Center for Privacy Protection Schleswig-Holstein, Germany, the Spanish Data Protection Agency and the Data Protection Commissioner of the Canton Zug, Switzerland, the International Conference resolves that:

Radio-frequency identification (RFID) technology is increasingly being deployed for a variety of purposes. While there are situations in which this technology can have positive and benign effects, there are also potential privacy implications. RFID tags are so far primarily used to identify and manage objects (products) to control the supply chain or to protect the authenticity of the product brand; however, they could be linked with personal information such as credit card details and even used to collect such information, or to locate or profile persons possessing tagged objects. This technology could allow for the tracing of individuals and for linking collected information with existing databases.

The Conference highlights the need to consider data protection principles if RFID tags linked to personal information are to be introduced. All the basic principles of data protection and privacy law have to be observed when designing, implementing and using RFID technology. In particular

a) any controller – before introducing RFID tags linked to personal information or leading to customer profiles – should first consider alternatives which achieve the same goal without collecting personal information or profiling customers;

b) if the controller can show that personal data are indispensable, they must be collected in an open and transparent way ;

c) personal data may only be used for the specific purpose for which they were first collected and only retained for as long as is necessary to achieve (or carry out) this purpose, and

d) whenever RFID tags are in the possession of individuals, they should have the possibility to delete data and to disable or destroy the tags.

These principles should be taken into account when designing and using products with RFID.

The remote reading and activating of RFID tags, without any reasonable opportunity for the person in possession of the tagged object to influence this process, would raise additional privacy concerns.

The Conference and the International Working Group on Data Protection in Telecommunications will monitor closely the technological developments in this field in greater detail in order to ensure the respect for data protection and privacy in the context of "ubiquitous computing".

**Explanatory Note:**

Radio-frequency identification tags (RFID tags) are currently being tested and increasingly being used as a more advanced form and possible replacement of bar codes ("smart labels"). The size of these microchips is about 1/3 of a millimetre (and smaller – "smart dust"). Most of them operate as passive transponders (without batteries) by listening to radio signals sent by transceivers (RFID readers) and using the energy of the received radio signal to reflect and answer it. Active RFIDs have a greater range (depending on the readers used). Since prices for RFID microchips and readers are dropping their widespread deployment becomes increasingly economically viable. RFID tags are likely to become essential drivers of ubiquitous (or pervasive) computing. Due to their storage and capacity for interactive communication they are far more powerful than bar codes. In addition they provide for unique identification of each tagged unit whereas bar codes are identical for every unit of the same product.

RFID tags can be used to install "smart shelves" in stores in order to better manage the supply chain and facilitate the replenishments of goods or supplies (e.g. the case of Gillette razors). They may also be used for easy (contact-less) payment at the point of sale especially if linked with credit cards. Furthermore an employer may use the technology to tag his property in order to reduce theft by employees. They could be linked with video surveillance cameras to check employee as well as customer behaviour. Specific documents may be tagged to be traced more easily in an office. Identity cards as well as travel documents (passports, visas) may be equipped with RFID tags. More recently the European Central Bank has announced that Euro notes will be issued with RFID tags in order to fight counterfeiting and money laundering as well as to control circulating notes. Washable RFID tags can be embedded in clothes ("wearable computing") in order to prevent or detect counterfeiting of specific brands and to prove the authentic manufacture of the product. Other possible applications range from car keys (immobilizers) to container management.

The RFID technology has numerous privacy implications. This is obvious in the case of implanted microchips But also in the more widespread case of tagged objects and goods undoubtedly the information transmitted also refers to the person carrying or wearing (or otherwise associated with) a tagged item or a "constellation" of brands thereby revealing the individual's taste. Therefore personal data can be processed and transmitted or read with the help of RFIDs or at least such object-related information can easily be linked with personal information (e.g. when a credit card is used for buying the tagged item). RFID tags have the potential of tracking the movements of a person who possesses or handles tagged objects.
Plans to afford technical devices legal protection against circumvention may prevent data subjects from disabling or deactivating RFID tags which function in a privacy-unfriendly way (e.g. after having paid and left the shop).

*Since this issue has led to a growing public debate in a number of countries it is recommended that the International Conference addresses the related privacy problems at this stage in order to encourage privacy-friendly solutions which have been proposed. The International Working Group on Data Protection in Telecommunications at its 34th meeting in Berlin on September 2 and 3, 2003, has expressed its support for this proposal.*

**Attachment H**

Safety Requirements.
A Task for the Data Protection Commissioners?

1. The Belgian law on data protection foresees technical and organisational measures to be taken by the data controller with regard to the protection of personal data.

This is along the lines of the European directive 95/46, that the Belgian law intends to transpose at national level.

Other texts re-state more or less this formula by clarifying even a little the aforementioned measures: Schengen agreements, the Safe Harbor, or the guidelines of the OECD governing the protection of privacy, and the cross-border flows of personal data.

Data controllers have the right to expect explanations on this subject from advisory and control authorities. And yet, there is no Decalogue on the matter. Even worse, there cannot be one, each processing and each information system having its characteristics and specific requirements, in particular according to the nature of the processed data.

How to get out of it?

2. The private sector did not hesitate to try to fill the gap by means of the global safety concept. It enacts standards of the type ISO, CEN or other. It grants labels guaranteeing the conformity of the information system to the aforesaid standards. It organises training with certification for the persons responsible for global safety.

A recent tendency takes shape, seeking to integrate in the global concept the security of data, and of personal data in particular.

Of course, one can be delighted of such initiatives, since they seek to fill a gap. But can we be satisfied? Can the advice and control authorities that we represent, consider themselves discharged from their mission and rely on these private initiatives?

Are these private initiatives sufficiently independent of the economic interests concerned or, on the contrary, don't they have their roots in these environments? And thus, in a facile but quivering way: are those who can be subject to controls the ones who determine their own standards and choose, by elaborating and certifying them, their controllers?

3. Let us not caricature, but concentrate on the role that the advice and control authorities can and must play.

Our role is legitimate only if it is limited to the standards regarding the security of personal data, in order to integrate our protection principles. The global safety concept concerns us only indirectly.

3.1. We have to ensure that the designers of the safety requirements are sufficiently representative of all those involved in the sector concerned and that they are not reduced to a professional association defending corporatist interests, where the main economic actors pull the strings, in relation to their economic weight.

3.2. We have to accompany, or even precede these designers by proposing more protective standards for the personal data of workers, customers, prospects, of the population samples concerned, etc...

3.3. We have to get involved in the process of granting of any safety or quality label within the framework of the two concerns referred to above: the designers' representatively and their accompaniment.

4. Security is a business which can be learned. How? On the job? In a corporatist cocoon in the pay of the main economic actors? Or on the contrary in universities and high schools, which have to envisage in their programs courses with contents and tenure guaranteed by the scientific community? To put the question is to answer it.

The business actors are certainly not to be excluded from this process. Their experience is an essential starting point. Their collaboration with the academic world is necessary. But the experience in this case has to find a guarantee in the scientific world, which has to be independent of the laws of the market.

Our data protection authorities have to persuade the persons responsible for higher education and all the actors concerned than such way is the most respectful of the rights and freedoms of all.

5. It is among the laureates of such teaching that the persons responsible for safety (both global and specific to data protection) have to be recruited.. Our authorities could contribute to the certification of these experts, certainly while awaiting the implementation of an official teaching. There are examples of such implication of the control authorities, inter alia in Belgium to approve the persons responsible for safety as regards Social Security data flows.

Insofar as standards are supranational regarding their process of elaboration, it appears obviously necessary that all the here recommended actions are carried out in co-operation between national authorities in order to guarantee, by their homogeneity, authority and effectiveness.

6. These are some ideas which I consider of particular importance and that I wanted to share with you. I know that I'm flirting (euphemism) with ideologies, cultures, customs. But I do not want to consider us as placid observers at a five-bar gate or wrapped up in our dear studies in our gilded cages.

Sydney, September 2003
Paul THOMAS,
President of the Belgian Data Protection Commission.