STEERING GROUP ON REPRESENTATION BEFORE INTERNATIONAL ORGANISATIONS

ANNUAL REPORT 2008/09

First report of the Steering Group
September 2009

/A207825

Contents **Page**

Executive Summary

The 30th Conference established the Steering Group on Representation before International Organisations. The Steering Group has the task of arranging observer representation before relevant international meetings in order to influence international data protection policy formulation and to keep the Conference better informed.

A full annual report outlining the Steering Group's activities and achievements will be made available on the Conference website.

A major initial task was settling the Steering Group's processes and working arrangements. The principal achievement was the adoption of the 'Expectations of Delegates' document. This is a guide to the key aspects of representing the Conference before international organisations.

During the year the Steering Group applied for observer status before four international organisations. The Conference:

- received Liaison Officer status before **ISO** in May - the Steering Group appointed Steve Johnston from Canada to the role;
- was granted guest status to observe the July meeting of the **APEC** Data Privacy Subgroup in Singapore - Billy Hawkes from Ireland was appointed as delegate;
- was recognised as an observer to the **Council of Europe** Consultative Committee on Convention No.108 in August. Allesandra Pierucci from Italy was appointed as the Conference's delegate to the plenary session in September.

An application to be an observer before the **OECD** Working Party on Information Security and Privacy has been submitted and a decision is pending.

The Steering Group has established contact lists for DPAs that wish to receive delegates' reports. To be added to the lists, please contact the Office of the Privacy Commissioner, New Zealand.

The Steering Group has proposed two resolutions to the Conference:

- the first seeks directions to obtain observer status before the Internet Governance Forum, London Action Plan (on spam) and ICANN;
- the second proposes a process for approving international organisations to be observers to the Conference's closed session.

Introduction by Steering Group Chair

I am honoured to present the first Annual Report of the Conference's Steering Group on Representation before International Organisations.

In order to influence international data protection policy formulation the Steering Group has the task of arranging observer representation before relevant international meetings.

The Steering Group is the culmination of a series of resolutions. It represents a determination by the Conference to translate talk into action

The Steering Group's origins are found in a resolution adopted 6 years ago at the 25th Conference. That resolution noted that 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. International requirements can cause difficulties at national level if the data protection dimension has not been considered during the international standard setting process. The resolution encouraged international bodies to develop processes by which privacy considerations could be factored into their work.

Three years later the London Declaration recognised that DPAs must develop coordinated strategies so as to act in new, more effective and relevant ways and in particular, to obtain institutional recognition of their action at the international level. The Working Group on Conference Organisational Arrangements reported back the following year suggesting that the Conference seek to influence international data protection policy formulation by obtaining observer status at meetings of international organisations. After a further study, the resolution establishing the Steering Group was adopted at the 30th Conference.

Thus the Conference has recognised the essential need to work collaboratively to influence matters at global level. It has never been sufficient to try to solve data privacy issues solely at national level. We are working innovatively to develop new structures to achieve data privacy goals. Collective statements of objectives and principles are essential but are not enough. There is the need to harness the expertise possessed within our DPA community and make it available to help find solutions to the complex and far reaching challenges in our global economy. The Steering Group is a practical step in this direction.

It has been a productive year for the Steering Group. The group has settled a number of fundamental process and organisational issues. However, while much can be achieved by the structures of the Steering Group and the dedication and hard work of the delegates, we will reach a point where some of the organisational challenges identified by the London Declaration will need to be directly addressed. The mooted Conference website will be a key tool. Before long the establishment of a Conference secretariat may need to be seriously explored.

The Steering Group has achieved a considerable amount in a comparatively short space of time. As a result of achieving observer status before important international organisations, this Conference is becoming recognised as an important player at international level.

The Steering Group has carefully prioritised its work. It has also identified new opportunities for engagement at international level in some challenging areas related to internet governance and enforcement. I commend the two resolutions to all DPAs.

I take this opportunity to thank all those involved in the work during the year. I offer special thanks to those individuals who have volunteered to be Conference delegates and to their employers. The current initiative will fail unless DPAs are willing to release staff for these duties.

There is opportunity for staff within DPAs to become further involved in this international work. I encourage any office that wishes to follow the work more closely, to place themselves on the relevant email circulation lists. There is also opportunity for those with special expertise to offer themselves to be delegates or alternate delegates.

Members of the Steering Group were elected for two year terms. I have been advised that all 10 current members will continue into their second year. While 10 members is quite sufficient for our work, there is opportunity if others wish to offer themselves for election.

Marie Shroff
New Zealand Privacy Commissioner
Chair, Steering Group

Report on activities for 2008/09

Establishment of Steering Group

The inaugural Steering Group included the 12 data protection authorities that proposed and co-sponsored the resolution adopted at the 30th Conference. New Zealand was chosen to lead the Steering Group. Each participating authority nominated a contact person and the resulting contact group conducted its work through exchange of emails. On specialist issues, small working groups of 3 or 4 members developed recommendations for the full group.

Members of the Steering Group, contact group and working groups are listed at Annex A:.

Steering Group's approach to tasks

The resolution establishing the Steering Group sets out basic arrangements for the Steering Group (see Annex B:).

The Steering Group spent many months considering the approach it should take to the work. This involved a mixture of fundamental issues, such as the process for mandating delegates, and practical issues, including priorities for 2009.

A major priority for the Steering Group was settling its processes for arranging representation. The 'Expectations of Delegates' document, which records key approaches, was finalised in April 2009 and circulated to all DPAs in July (see Annex C:).

2009 priorities

The Conference resolution directed the Steering Group to seek observer status before seven international organisations. The Steering Group gathered information about the data privacy work of the international organisations, their committee structures and key contacts and other useful information. As a result, the Steering Group decided to approach the task in the following order:

- first priority: ISO, APEC, OECD;
- second priority: Council of Europe;
- third priority: ITU, ILC and UNESCO.

ISO

ISO had earlier invited the Conference to appoint a liaison officer. Accordingly, the Steering Group moved quickly to take up this opportunity. An application was made to ISO in April 2009 and Steve Johnston, from Canada, was appointed as delegate. ISO approved the liaison officer arrangement in meetings in Beijing in May and the occasion was marked by a joint news release (see Annex D:).

APEC

Having explored the issues and taken advice, the Steering Group submitted an application for guest status before both the Data Privacy Subgroup (DPS) and its parent committee, Electronic Commerce Steering Group (ECSG). The ECSG application was opposed and so we asked for the DPS application to be considered alone. We had hoped to obtain guest status for a period of two years (covering four meetings). However, only a single meeting

approval was granted. We understand this to be quite usual and have been encouraged to resubmit an application for a two year approval. Billy Hawkes, from Ireland, was appointed as delegate to the Singapore meeting in July.

Council of Europe

The Steering Group applied for observer status before the Council of Europe Consultative Committee and Bureau in July. Approval was obtained in late August just one week before the annual plenary meeting. Accordingly, interim arrangements were made to secure a delegate for that meeting. Allesandra Pierucci, from Italy, was appointed as delegate to the September meeting.

OECD

Having taken soundings from the OECD Secretariat, the Steering Group decided to seek observer status rather than the alternative 'expert' status. An application was submitted in July and is due to be considered by the OECD WPISP meeting in October, after the finalisation of this report.

ITU, ILC, UNESCO

The Steering Group has a mandate to seek representation from three further organisations - International Telecommunications Union (ITU), International Law Commission (ILC) and UNESCO.

After initial exploration of the issues, the Steering Group does not intend to seek representation before ITU, ILC or UNESCO in the short term but hopes to reconsider all three in 2011. In particular, the ILC is not expected to commence its privacy reference during 2010. It does not appear feasible to undertake ITU work before 2011. The Steering Group has not identified sufficient value to become engaged in UNESCO's work at this time.

New directions sought: IGF, LAP, ICANN

The basic arrangements direct the Steering Group to research the international scene to identify opportunities for useful participation. Three bodies have been identified for possible further engagement:

- Internet Governance Forum (IGF);
- London Action Plan (LAP) (against spam);
- Internet Corporation for Assigned Names and Numbers (ICANN).

The Steering Group recommends that the Conference direct the Steering Group to explore seeking representation before these organisations (see resolution at Annex H:). More careful exploration of the issues will need to be undertaken and it may transpire that, on closer examination, observer status is not warranted before all three. Seeking representation will also be dependent upon the Steering Group being confident that it can identify a representative from a DPA willing to be the delegate.

Resolution on international observers before closed sessions

The basic arrangements direct the Steering Group in its first annual report to recommend any necessary or desirable improvements to the basic arrangements. The Steering Group reviewed the basic arrangements and was satisfied that they did not at this stage require any

changes. However, the Steering Group does recommend the adoption of a new process for admitting observers from international organisations to the closed session of the Conference (see second resolution at Annex I:).

DPA involvement in international work

There are several opportunities for interested DPAs to become involved in the international work. The opportunities include to:

- Become a member of the Steering Group – while the Steering Group has sufficient members are present, up to 5 additional DPAs could be elected at the 31 Conference;
- Become a delegate or alternative delegate - the Steering Group is willing to consider *ad hoc* delegates for single meetings of the regional organisations (including the Council of Europe and APEC) and there are openings for alternate delegates to back up appointed delegates;
- Join the distribution lists - any DPA that wishes to follow the work of one or more of the organisations or to offer feedback to the delegates is encouraged to provide email details to be added to the appropriate lists (contact: Linda.williams@privacy.org.nz).

Observation on the year

The Steering Group is pleased with the progress during the year. Foundation work has been completed to establish the Steering Group's processes and approaches to the work. Submitting four applications for observer status has been a substantial accomplishment. The community of DPAs now has a recognised presence before several influential international organisations.

While it is too early to evaluate the effectiveness of the observer arrangements, the processes appear to be working as anticipated. A window into the work of international organisations has been provided for the Conference.

Annex A:

Steering Group

Steering Group Chair:	Marie Shroff, New Zealand
Steering Group Authorities:	Australia, Berlin (resigned March 2009), Canada, European Data Protection Supervisor, France, Germany, Hong Kong, Ireland, Italy, New Zealand, Spain, Switzerland (resigned February 2009)
Principal contacts:	Timothy Pilgrim (Australia), Carman Baggaley (Canada), Peter Hustinx (EDPS), Gwendal Le Grand (France), Silke Harz (Germany), Roderick Woo (Hong Kong), Gary Davis (Ireland), Antonio Caselli (Italy), Blair Stewart (New Zealand), Rafael Gozalo (Spain)
ISO Working Group:	Carman Baggaley, Gwendal Le Grand, Silke Harz, Blair Stewart
APEC Working Group:	Carman Baggaley, Timothy Pilgrim, Blair Stewart Roderick Woo
OECD Working Group:	Carman Baggaley, Gwendal Le Grand, Silke Harz, Blair Stewart
Council of Europe Working Group:	Antonio Caselli, Blair Stewart, Roderick Woo

Delegates

ISO Liaison Officer:	Steve Johnston, Canada (appointed May 2009)
APEC Guest:	Billy Hawkes, Ireland (appointed for meeting of 28 July 2009)
Council of Europe Observer:	Allesandra Pierucci, Italy (appointed for meeting of 2–4 September 2009)

Annex B:

Resolution adopted at the 30th Conference Establishing the Steering Group on Representation at Meetings of International Organisations

The 30th International Conference of Data Protection and Privacy Commissioners

Recalling and noting:

(a) the resolution of the 25th Conference that called upon international bodies to adopt suitable mechanisms to ensure that data protection considerations are taken into account when promulgating standards, rules or common practices that affect personal data handling within national jurisdictions

(b) the Montreux Declaration adopted at the 27th Conference which resolved to strengthen collaboration with international organisations

(c) the 28th Conference's London Declaration which called for Data Protection Authorities to bring forward coordinated strategies to act in new and more effective ways and, in particular, to obtain better institutional recognition at the international level

(d) the resolution of the 29th Conference that outlined a process to influence international data protection policy formulation by obtaining observer status at meetings of international organisations

(e) the resolution of the 29th Conference on Development of International Standards which encouraged the Conference to find ways to pool the collective expertise of Data Protection Authorities and to make that expertise available to ISO in the development of privacy standards

Therefore resolved:

1. To create a process to enable collective contribution to the work of international organisations and representation of Data Protection Authorities at meetings of international organisations, both governmental and non-governmental, in order to better promote the basic universal principles of data protection and privacy at international level, and

2. To establish a Standing Committee of the Conference to be known as the Steering Group on Representation before International Organisations, to be operated in accordance with the basic arrangements set out in the annex to this resolution, and

3. To elect an inaugural Steering Group, and

4. To direct the inaugural Steering Group to explore the usefulness of obtaining observer representation, and if appropriate to obtain such representation, at the meetings of the appropriate committees or working groups of the following international organisations:
    a. OECD
    b. International Organisation for Standardisation

c. Council of Europe
d. APEC
e. International Law Commission
f. International Telecommunications Union
g. UNESCO.

In addition to the international organisations listed above, if the Steering Group considers appropriate and useful to do so, the Steering Group may seek and obtain representation at the meetings of the appropriate committees and working groups of other international organisations, in accordance with the process set out in clause 2d of the annex.

ANNEX

Basic arrangements for the Steering Group on representation before International Organisations

1. Membership

a. Membership of the Steering Group will be by:
- election by accredited Data Protection Authorities (DPAs) at the closed session of the Conference, or
- co-option by the Steering Group between Conferences (in the limited circumstances set out in clause 1d).

b. Any DPA accredited to the Conference may be elected to, or co-opted onto, the Steering Group.

c. The Steering Group must include between 5 and 15 DPAs.

d. The Steering Group should, if possible, include members from the various regions of the world. Between Conferences the Steering Group may co-opt up to 2 DPAs to ensure continued broad coverage.

e. The term of elected Steering Group members is 2 years. Members can resign before the end of their term and may be re-elected as often as they wish. The term of a co-opted member is until the date of the next Conference.

2. Directions concerning international organisations

a. The resolution establishing the Steering Group directed the Steering Group to seek observer representation (or similar status) from an initial six international organisations.

b. The Conference may from time to time direct the Steering Group to seek representation before other international organisations.

c. One of the Steering Group's functions is to identify useful opportunities for representation and to make recommendations to the Conference seeking directions to obtain representation.

d. The Steering Group may proceed to seek representation before other international organisations in the absence of directions from the Conference. However, the Steering Group must first obtain indications of support for such action from at least half of the DPAs accredited to the Conference.

3. Working methods

a. The Steering Group will elect its own chair.

b. The Steering Group will settle its own procedures, document them and communicate them to members of the Steering Group and other DPAs.

4. Functions of Steering Group

a. The Steering Group will have the functions set out in this and other clauses and any additional functions conferred by resolution of the Conference.

b. The principal functions of the Steering Group will be to:

i. Research the international scene to identify opportunities for useful participation.

ii. Pursue applications to obtain observer status at appropriate international meetings.

iii. When status has been granted, to arrange for one or more DPAs to be the Conference's delegate.

iv. Develop and document the approach of the Steering Group to mandating delegates.

v. Provide general or specific guidance to Conference delegates.

vi. Receive reports from delegates.

vii. Provide reports to the Conference.

c. In addition to any additional reports that the Steering Group thinks useful to make, the Steering Group shall provide the following reports:

i. An annual written report to the Conference about the Steering Group's activities including an account of any observer representation sought or granted, delegate appointed and meetings attended.

ii. The first annual report should include an account of the operation of the resolution establishing the Steering Group including these basic arrangements and recommend any necessary or desirable improvement.

iii. Recommendations as to any additional international organisations for which a direction should be given to the Steering Group.

5. Delegates

a. The Steering Group must establish processes for appointing delegates generally or in a specific case.

b. The Steering Group may appoint any DPA as a delegate whether or not that DPA is a member of the Steering Group.

c. Appointment as a delegate may be for a specific meeting or for a specified period of time. Time-based appointments should be reviewed or renewed periodically.

d. The Steering Group will provide general guidance for delegates.

e. All resolutions of the Conference are to be considered a standing direction to all delegates.

f. As part of its practices of providing general or specific guidance to delegates, the Steering Group must develop processes for soliciting views from affected DPAs in appropriate cases. "Affected DPAs" may include:

- DPAs from countries or economies that are members of the international organisation in question;
- all DPAs in some cases.

6. Expenses

a. The Conference is not liable for any expenses of the Steering Group, its members or delegates.

b. The Steering Group is not liable for any expenses of members or delegates.

Annex C:

Expectations of Delegates

The International Conference of Data Protection and Privacy Commissioners encourages individuals within accredited data protection authorities (DPAs), both commissioners and staff, to offer themselves to be the Conference's observer to meetings of particular international organisations. Volunteering as observer (referred to in this note as 'delegate') involves devoting some time and expense to work on behalf of the Conference. The Steering Group is grateful to DPAs, and the individuals concerned, for performing such services. To assist authorities to decide whether to release staff (or commissioners) for the task, and to help the individuals concerned, this note outlines the Steering Group's broad expectations of delegates.

General expectation
The delegate will be an expert in data protection and privacy and knowledgeable in the work of both the Conference and the international organisation. The delegate will be Conference's 'eyes and ears', attending and observing the international organisation's meetings and reporting relevant information back. The delegate will be an advocate for data protection and privacy and, while taking care not to purport to speak on behalf of the Conference in the absence of an applicable resolution, will articulate data protection and privacy positions when the opportunity is given. The delegate will self-manage the relationship between the Conference and the international organisation by processing the available information, identifying the opportunities and risks and advancing the Conference's objectives.

1. Expertise

The Steering Group will presume that all nominees for a delegate role from DPAs will possess a good knowledge of data protection and privacy theory and practice.

Delegates should be familiar with the principal international instruments governing data protection and privacy regulation. The delegate's knowledge should extend beyond the guiding instruments governing the law in the delegate's own jurisdiction to include the other major instruments around the world.

Delegates are expected to be familiar with the relevant resolutions adopted by the Conference.

Delegates are expected to have a reasonable working knowledge of the relevant work of the international organisation concerned or be willing to familiarise themselves upon being appointed. Nominees for the role of delegate will be asked to complete a form for the Steering Group outlining previous experience relevant to the work of the international organisation.

Delegates will need to familiarise themselves with the relevant processes of the international organisation including any special rules applicable to observers.

2. Attendance at meetings

It is expected that prospective delegates will give the Steering Group a realistic estimate of their availability to travel to and attend the relevant meetings during the period of appointment. Ideally delegates will be likely to be able to attend all or nearly-all of the important meetings of the relevant international organisation or committee during the expected term of the appointment.

However, firm commitments to attend all or nearly-all meetings are not always realistic or even necessary. In some cases, the role of delegate may require attendance at only a selection of meetings with other meetings to be followed 'on the papers'. If an alternate is also appointed, it will be sufficient to ensure a reasonable coverage of meetings between delegate and alternate. Occasionally, an alternate delegate will be appointed simply to attend a single meeting, sometimes in cases where the principal delegate cannot attend.

Delegates are expected to assess which of the forthcoming meetings warrant attendance. Delegates should keep the Steering Group reasonably informed of their assessments and be willing to explain their views.

Where the delegate assesses that a meeting should be attended, it is expected that the delegate will:

- attend the meeting, or
- arrange for the alternate (where appointed) to attend, or
- in cases where neither the delegate nor alternate can attend, let the Steering Group know the position in plenty of time with a recommendation, if possible, of a prospective candidate for the Steering Group to appoint as a delegate to attend the particular meeting.

Where the delegate assesses that a meeting need not be attended, or where attendance is simply not able to be arranged, the delegate is expected to convey the Conference's apologies through appropriate channels.

It is accepted that some delegates will attend some meetings in the dual capacity of Conference observer and as a member of a national delegation. This may be unavoidable as cost constraints will otherwise often prevent DPAs from attending without this combination of roles. However, the Steering Group expects delegates to manage the dual role so as to reflect well on the Conference and avoid any conflicts. In particular, it is expected that delegates will:

- let the Steering Group know if they propose to attend meetings in this dual capacity;
- ensure that the appropriate officials responsible for the meetings know of their dual capacity;
- ensure that there is no confusion as to the capacity in which they are intervening during meetings;
- ensure that their reports to the Steering Group reflect a Conference, rather than national, perspective.

3. Following the international organisation's work

Delegates are expected to follow closely the relevant work of the international organisations. Delegates will need to arrange to receive and read the relevant papers.

Delegates are not expected to be an expert in every aspect of the relevant work of the international organisations. However, delegates should have a reasonable knowledge of the relevant organisation's work, be a reliable source of information for the Conference on that work and to be able to obtain further information if asked.

Delegates will also be expected to be able to assess and interpret what they know of the international organisation's work so that they may bring significant privacy and data protection issues to the attention of the Conference.

4. Keeping others informed

Delegates are expected to keep the alternate and the Steering Group informed of their activities as delegate and to keep the Steering Group, interested DPAs and the Conference informed of the work of the international organisation.

If an alternate is appointed a delegate must keep the alternate appropriately informed. Typically, this will involve ensuring that the alternate has access to the necessary papers and knows of the delegate's plans in relation to meetings. The degree to which the delegate needs to keep the alternate informed will vary and this is a matter to be worked out between the delegate and the alternate. Delegates should try to ensure that the alternate is in a reasonable position to assume the delegate's responsibilities in the event that the delegate is unable to attend a meeting.

Delegates are expected to keep the Steering Committee reasonably informed. Delegates should provide sufficient information to reassure the Steering Group that the observer arrangements are working satisfactorily or to highlight any problems arising or matters requiring guidance from the Steering Group. Delegates are expected to produce some written reports for the Steering Group, in particular, material for incorporation in the Steering Group's annual report to the Conference.

Delegates are expected to maintain networks of, and provide reports to, interested DPAs who wish to follow the work of the international organisation. The arrangements for doing this may differ between organisations and delegates. Generally speaking it may involve delegates establishing and maintaining an email contact list of staff within DPAs who have asked to be kept informed. Delegates are expected to prepare and distribute short update reports at appropriate intervals (typically preceding and/or following important meetings). Sometimes the update report may include relevant documentation from the international organisation, such as meeting minutes or resolutions, where circulation of such documentation is permitted.

Delegates are expected to hold themselves open to answer questions from any DPA and the Steering Group about the work of the international organisations.

There may be opportunities for delegates to report back on the work of the international organisations at the annual conference. Such opportunities cannot be guaranteed given the pressure on the Conference programme but where such opportunities are available, and delegates are able to attend the Conference, it is expected that delegates will be willing to provide a presentation or answer questions.

5. Representing the Conference

The delegate's role is, first and foremost, as an observer. The international organisation will have granted the Conference privileged access to attend meetings not open to the public. Delegates observe, interpret and report back to interested DPAs and the Conference.

In accordance with the particular arrangements of the international organisation, delegates may also be able to do various other things. This might vary depending upon the nature of the meeting and the rules of the particular organisation. Typically, there will be a process whereby observers may be allowed to intervene in some part of proceedings, for example, to make a statement or ask a question. Sometimes participants might ask a question of observers.

It is expected that delegates will exercise careful judgment in preparing for and participating in the meetings to ensure that the participation provides most value to all concerned. Delegates must take care to avoid expressing positions on behalf of all DPAs or the Conference unless they have a mandate to do so. Where the Conference has adopted a resolution on a particular matter, this can be represented as a clear mandate. In the absence of a Conference resolution, expressions of view may best be stated at a sufficiently high level, in keeping with well understood and agreed principles of data protection and privacy, or expressed as an expert but personal view.

On occasion, a delegate will know in advance of a meeting that an international organisation will wish to hear an expression of views. In those cases, the delegate may wish to consider preparing a brief written statement of position in advance. In the absence of a Conference resolution this should not be stated to represent the view of the Conference but with the right preparation may be characterised as a position said to be generally in keeping with the views of DPAs attending the Conference. Such a statement should be accompanied by a suitable caveat to the effect that the Conference has not taken a resolution on the point.

If proposing to prepare such a statement, it is expected that delegates will seek views from other DPAs. The alternate is the primary resource to assist in this respect. The circulation list developed to keep interested DPAs informed is the second resource. The third resource is the Steering Group itself which is available for consultation and guidance and will wish to see statements that may be proposed to be tabled. In some instances, a matter could be raised with all DPAs (and the Steering Group has a circulation list for such use). However, to ensure proper coordination the delegate should not usually canvass views of all DPAs except through the Steering Group or with the Steering Group's approval.

In some instances, delegates may identify issues on which it will be helpful for the Conference to adopt a resolution. Those issues may be fed through the Steering Group to be considered as part of a Steering Group-sponsored resolution. This does not preclude a delegate's own DPA proposing a resolution of its own initiative.

6. Identifying opportunities

Delegates are encouraged to use their initiative to further the objectives of the Conference and of privacy and data protection generally. In particular, delegates are expected to take any opportunity offered to observers to provide an update to the international organisation on the work of the Conference.

Other opportunities may present themselves. For example, delegates may wish to encourage key people within the international organisation to attend the public sessions of

the Conference. Delegates may also be a resource to Conference hosts in identifying or approaching possible speakers for Conference sessions.

7. Duration of appointment as delegate

An appropriate term of appointment will be made which may depend upon the delegate's preferences and availability and the nature of the international organisation and the particular series of meetings. In judging appropriate terms of appointment the Steering Group will try to ensure that while delegates are able to develop expertise in their role and perform effectively there remain opportunities for as many DPAs to contribute as possible.

As a general matter, delegates are expected, if possible, to make themselves initially available for a two year appointment which may be the normal duration. A renewal for up to a further two years will be contemplated but at the completion of an extended term it is expected that a delegate may step aside if there is another candidate offering themselves as delegate. The Steering Group will invite expressions of interest from the Conference at large for available positions from time to time.

It is expected that delegates will help ensure an orderly transition from one delegate to the next. The Steering Group would appreciate as much notice in advance as possible if delegates do not intent to continue in the role. Assistance in finding a successor, and briefing that person, will be appreciated.

Delegates should promptly advise the Steering Group if their employment by, or appointment to, a DPA ends. Delegates are expected to step down if asked to do so by the Steering Group.

The Steering Group may revoke an appointment if a delegate significantly fails to meet the expectations set out in this document or gives other cause for removal.

Version 1.1
Adopted by the Inaugural Steering Group comprising DPAs from Australia, Canada, France, Germany, Hong Kong, Ireland, Italy, New Zealand, Spain and the European Data Protection Supervisor
Date: 26 August 2009

Annex D:

Joint ISO/Steering Group news release: May 2009

International Conference of Data Protection and Privacy Commissioners cooperates with ISO in developing International privacy standards

IS THERE A SOLUTION ON THE HORIZON TO COMBAT THE THREAT TO OUR DATA PROTECTION AND PRIVACY?

13 May 2009: The threat to the protection and privacy of our data has been a challenge faced by citizens, regulators and organisations around the world for many years. The threat is growing at an alarming rate and will continue to do so unless some international solutions are found to combat this problem.

A significant step towards achieving an international solution took place today with a joint announcement by Marie Shroff, the New Zealand Privacy Commissioner and Walter Fumy, the Chairman of ISO/IEC JTC 1/SC 27, the leading international standards committee on information security.

Commissioner Shroff announced that the International Conference of Data Protection and Privacy Commissioners had appointed Steven Johnston, Senior Security and Technology Advisor to the Office of the Privacy Commissioner of Canada, as liaison officer SC 27's WG 5 on identity management and privacy technologies.

The New Zealand Commissioner chairs the International Conference's Steering Group on Representation before International Organisations, which was established at the 30th Conference in Strasbourg late last year.

Commissioner Shroff said:

> *"The establishment of the Steering Group was a major step forward for the Conference by creating a mechanism by which the collective privacy and data protection expertise of commissioners could be better linked into international policy formulation. This appointment is a practical manifestation of that initiative.*
>
> *There are now many players in the international scene working to develop solutions to the privacy challenges facing the world. The Conference's initiative is one small step to link together some of the stakeholders to share knowledge and experience. Steven Johnston has a depth of experience in relation to security, technology and the standards process that will serve the Conference and WG 5 well."*

Dr Walter Fumy said:

> *"I warmly welcome this collaborative development with the International Conference of Data Protection and Privacy Commissioners. It represents an important turning point in advancing data privacy and protecting personal information through the publication of international privacy standards in the area of technology in the near future."*

Professor Kai Rannenberg, Convener of WG 5, said:

> *"I am very pleased to see this liaison become a reality as it is important for SC 27 to bridge the gap between Privacy Requirements and Privacy Technology. The threat to privacy affects everybody whether in healthcare, mobile communications or social networks. The nomination of Steven Johnston nicely complements the earlier appointment of Stefan Weiss as Liaison Officer from WG 5 to the Conference".*

Edward Humphreys, Press Officer, SC 27
Blair Stewart, Assistant Privacy Commissioner, New Zealand

All enquiries about this press release may be directed to edwardj7@msn.com for ISO/IEC JTC 1/SC 27 or to enquiries@privacy.org.nz.

For more details of this joint cooperation go to the ISO/IEC JTC 1/SC 27 web site http://www.jtc1sc27.din.de/en. Also contained on this web site is a full list of ISO/IEC JTC 1/SC 27 projects.

For further information about the International Conference of Data Protection and Privacy Commissioners, go to resolutions on global standards and appointing liaison officer or to this year's conference web site.

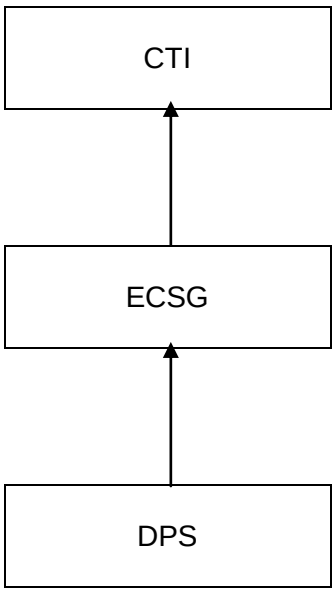
Annex E:

Delegate report: Asia Pacific Economic Cooperation (APEC)

Electronic Commerce Steering Group (ECSF) Data Privacy Subgroup (DPS)

Organisational Information

Mandate of committee:
The ECSG was established in 1999 to promote the development and use of electronic commerce by creating legal, regulatory and policy environments in the APEC region that are predictable, transparent and consistent. The Data Privacy Sub-group was established by the ECSG in 2003 initially to develop the APEC Privacy Framework which aims to provide a consistent approach to information privacy protection, avoid the creation of unnecessary barriers to information flows and prevent impediments to trade across APEC member economies. Following adoption of the Framework in 2005, the DPS has continued to coordinate work on data privacy including by providing technical assistance to APEC economies. The current major DPS focus is a Pathfinder on cross-border privacy rules.

Structure


Abbreviations:
APEC – Asia Pacific Economic Cooperation CBPR – Cross-border Privacy Rules CTI – Committee on Trade & Investment DPS – Data Privacy Subgroup ECSG – Electronic Commerce Steering Group

Conference representation

Observer status granted
July 2009 (for meeting of 28 July)

Observer
Billy Hawkes, Data Protection Commissioner, Ireland (for meeting of 28 July)

Meetings attended
Singapore, 28 July 2009

Delegate report

Background

The Sub-Group operates under the aegis of the APEC[1] Electronic Commerce Steering Group. It's main task is to facilitate and encourage implementation of the APEC Privacy Framework[2], which was approved by APEC Ministers in 2004. The Framework is designed to promote *a flexible approach to information privacy protection across APEC member economies, while avoiding the creation of unnecessary barriers to information flows*. The Framework is based on 9 APEC Information Privacy Principles[3]. The Framework includes guidance on how to give effect to the Principles, both domestically and internationally. 14 of the 21 Member Economies have published Data Privacy Individual Action Plans[4] which describe the state of implementation of the Framework.

In 2007, APEC Ministers approved a Data Privacy Pathfinder[5] with the aim of developing *a framework for accountable flows of personal data across the region, focussing on the use of cross-border privacy rules by business*. 9 Pathfinder Projects[6] have been designed. These

[1] APEC is a grouping of 21 "Member Economies" in the Asia-Pacific Region: Australia, Brunei Darussalam, Canada, Indonesia, Japan, Korea, Malaysia, New Zealand, the Philippines, Singapore, Thailand, United States, China Hong Kong, China, Chinese Taipei, Mexico, Papua New Guinea, Chile, Peru, Russia, Viet Nam.
[2] Available at: www.apec.org
[3] Preventing harm; Integrity of Personal Information; Notice; Security Safeguards; Collection Limitations; Access and Correction; Uses of Personal Information; Accountability; Choice
[4] Available at: http://www.apec.org/apec/apec_groups/committee_on_trade/data_privacy_iaps.html
[5] Available at: http://aimp.apec.org/Documents/2007/SOM/CSOM/07_csom_019.doc
[6] The 9 Pathfinder Projects are: self-assessment guidelines for organisations; private and public sector accountability agent recognition criteria; compliance review process of CBPRs (Cross Border Privacy Rules); directories of compliant organisations and contact information of organisations and accountability agents for use by consumers; contact directories for data protection authorities and privacy contact officers within economies, as well as with accountability agents; templates for enforcement cooperation arrangements; templates for cross-border complaint handling forms; scope and governance of the CBPR system, and a pilot program to test and implement the results of the projects leading to the testing of a complete system.

involve developing and testing the practical tools required to give effect to a Cross-Border Privacy Rules (CBPR) system. The 4 elements of the system are:

- Self-assessment – an organisation develops rules and procedures consistent with the APEC Privacy Principles
- Compliance Review – the organisation's rules are checked by an accountability agent for compliance with the APEC Privacy Principles
- Recognition/Acceptance – compliant organisations are placed on a list of participating organisations and will be recognised as such in the APEC region
- Dispute Resolution and Enforcement – domestic and cross-border procedures for resolving complaints, including by appropriate regulators

Implementation of Data Privacy Pathfinder Projects

This was the main item on the Subgroup's agenda. Significant progress was reported on all of the Projects. Of particular interest was a report on the testing of the CPBR model, using volunteer companies and private-sector accountability agents. Feedback from the testing phase may lead to a rethink of some details of the questionnaires used in the test.

There was a large degree of agreement on the practical and governance arrangements for making the CPBR system work. These arrangements include agreed criteria for mutual recognition of accountability agents, cooperation between Privacy Enforcement Authorities and designation of an Administrator of the system.

Capacity Building Activities

The Chair gave an oral report on a data privacy seminar which had taken place the previous day. The seminar involved presentations and discussion on a variety of data privacy topics, including developments in other regions and the meaning of "accountability". The Vietnamese delegation reported on a workshop which had taken place the previous week in his country, with the involvement of the US Federal Trade Commission and the US Centre for Information Policy Leadership. Further such workshops are planned, supported by the Subgroup.

Domestic Implementation of the APEC Privacy Framework

Malaysia, Mexico, Indonesia, Peru, Philippines, Chinese Taipei, Thailand and Vietnam reported that draft privacy legislation was at various stages of development. Russia expects to appoint a data protection authority under its existing legislation this year. Australia, New Zealand, Hong Kong China and Canada are reviewing their existing privacy legislation. In all cases, the legislation is expected to be consistent with the APEC Privacy Framework.

2010 Work Plan

Completion of the work on the CPBR system and further capacity-building activities, including in relation to domestic implementation of the APEC Privacy Framework.

Information Sharing on Cross-Border Privacy Issues

Reports were provided on developments in various regional and international bodies of relevance to cross-border privacy issues. The Subgroup wishes to develop a more active dialogue with such bodies. It was noted that a session involving APEC is planned for the Madrid Conference in November.

Annex F:

Delegate report: Council of Europe (T-PD)

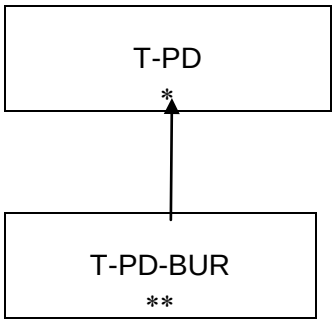
Consultative Committee of the Convention for the Protection of Individual with regard to Automatic Processing of Personal Data (T-PD) and the T-PD Bureau (T-PD-BUR)

Organisational Information

1. Name of Organisation
Council of Europe

2. Name of Committee
Consultative Committee of the Convention for the Protection of Individual with regard to Automatic Processing of Personal Data (T-PD)

3. Mandate of committee:
The Committee is a forum for policy making and standard setting under Convention 108 (Article 18) and to monitor trends, share experiences and information, analyse the impact of privacy protection. In particular, the Committee, under Article 19 of the Convention: • may make proposals to facilitate or improve the application of the Convention No. 108; • may make proposals to amend the Convention; • must formulate an opinion on any proposal for amendment of the Convention which is referred to it; and • may express an opinion on any question concerning the application of the Convention.
4. Composition:
Each Party of the Convention appoints a representative to the Committee and a deputy representative. Any Member State of the CoE which is not a Party of the Convention has the right to be represented o the Committee by an observer (Article 19 of the Convention). The Committee is composed by representatives of DPA or other institutions.

5. Structure (diagram)
 * See the Rules of procedure of the Consultative Committee.

** In accordance with art. 10 bis of its Rules of procedure, the Committee has established the T-PD BUR to prepare the meetings of the T-PD and in particular to prepare preliminary draft legal instruments, drafting opinions and reports, preparing the programme of activities and carrying out activities conferred on it by the T-PD.

Abbreviations:
T-PD: Consultative Committee T-PD-BUR: Bureau of the committee

Conference representation

Observer status granted
August 2009

Observer
Alessandra Pierucci, Data Protection Authority, Italy (for meeting of 2 – 4 September)

Meetings attended
Strasbourg, 2–4 September 2009

Delegate report:

General information
The meeting started with the usual information given by the Secretariat (Directorate General of Human rights and Legal affairs) of the Council of Europe. J. Polakiewicz welcomed the International Conference as an observer and updated delegates on the ratifications of Convention 108 and its Additional Protocol, recalling the main forthcoming events of interest for the participants - in particular the 31st International Conference of Data Protection and Privacy (Madrid 4-6 November 2009).

T-PD Work Programme
The plenary discussed and approved the T-PD Work programme for 2009 and beyond. Apart from the issue of "profiling" which will be referred later, the T-PD agreed to work on the following priorities: a) analysis of the Recommendation R(87)15 regulating the use of personal data in the police sector, in particular to determine the principles to be developed in order to cover adequately the emerging issues of data protection in the filed of prevention, investigation, detection or prosecution of criminal offenses or the execution of criminal penalties; b) updating of Recommendation (89)2 on the protection of personal data used for employment purposes, in light of technological developments as well as of other texts of the CoE containing provisions on the processing of data in the employment field. The T-PD, according to the approved Work programme, will also deal with the following issues: c) status and powers of data protection authorities in view of the drafting of an explanatory document setting out a "model" of the supervisory authority as foreseen by the Additional Protocol; d) carrying out a study in order to assess the need and added value of a fundamental right to data protection as distinct from Article 8 of the ECHR; e) carrying out an evaluation of social networking in view of possible initiatives; f) constant follow-up of

developments in data protection within and outside the CoE; g) preparation of the celebration of the 30th anniversary of signature of the Convention 108.

Data Protection Day
The T-PD agreed that the date of the Data Protection Day should remain as 28 January. It being understood that activities could be organised in the week around this date therefore preserving a certain amount of flexibility. This will not prevent States from organising data protection aware-raising activities during other dates.

Presentations and requests of observer status
The T-PD took note of the presentation and the request by the European Privacy Association for observer status within the T-PD. It took note of the presentation of the Ad hoc Committee for the World Anti-doping Agency (CAHAMA) and entrusted the Spanish representative J.L. Nuñez García with the task of representing the T-PD during the forthcoming meeting of the abovementioned Committee in Madrid on the 14th of September 2009. It also took note of the presentation of the "Group of specialists on predictivity, genetic testing and insurance" of the Steering Committee on Bioethics of the CoE and instructed the Secretariat of the T-PD to open a call in order to identify a possible T-PD member to join the Group.

Participants exchanged information on recent national developments in the field of data protection.

T-PD Statement on International Standards on the protection of privacy
The T-PD, as the forum for policy making and standard setting under Convention 108, examined the Joint Proposal for a Draft of International Standards on the protection of privacy" ("hereafter International standards") in view of the forthcoming Madrid International Conference. The T-PD adopted a Statement welcoming the International standards as a valuable action for the effective protection of privacy in an increasingly globalised world. The Statement recalls the importance of the standards contained in Convention 108 and its Additional Protocol (taken as one of the sources of the International standards) emphasising their legally binding nature, technological neutrality and applicability to privacy intrusions by public and private authorities. It recalls the CoE's Committee of Ministers' decision adopted on 2 July 2008 encouraging the accession of non Member States with the required data protection legislation and highlights that the T-PD counts on continued support of the International Conference in this kind of endeavour and on its active involvement in the T-PD activities as an observer. The Statement also points out that the International standards may help to interpret Convention 108 in the light of technological developments and even develop new legal instruments.
The Statement concludes that the International standards could lead to a new impetus to the strengthening of data protection and contribute to the worldwide promotion of Convention 108 and its Additional Protocol, therefore promoting harmonisation and reinforcement of the right to privacy in a global perspective.

Draft Recommendation on profiling
The second and third days of the meeting have been mostly dedicated to the analysis of the Draft Recommendation on the protection of individuals with regard to automatic processing of personal data in the framework of profiling.
A thorough discussion followed regarding the field of scope of the Recommendation, in particular whether the text should be either limited to the sole private sector or extended to the public sector, namely the fields of defense, national security and/or police and justice. The plenary decided to limit the scope to the private sector, however providing for the possibility for each Member state to extend such principles also to the public sector.

The plenary did not succeed in the adoption of the text also in consideration of the number of amendments that were brought as a result of the discussion. Therefore the redrafted text will be submitted to a final vote at the 2010 plenary.

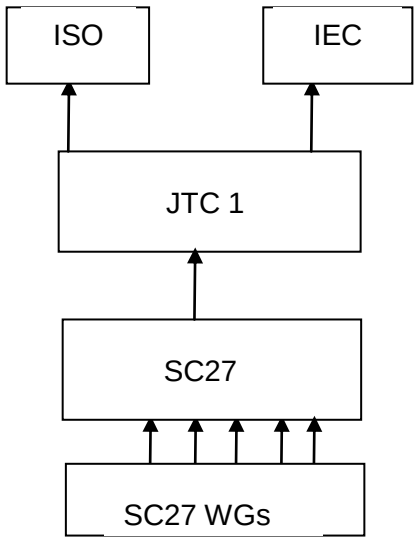
The plenary did not object to the request of the European Commission to circulate the text to the members of the Article 29 Group.

Annex G:

Delegate report: International Organisation for Standardisation (ISO) SC27/WG5

Organisational Information

Mandate of committee
The scope of SC27/WG 5 covers the development and maintenance of standards and guidelines addressing security aspects of identity management, biometrics and the protection of personal data. Current SC 27 projects include: • Framework for Identity Management (ISO/IEC 24760) • Biometric template protection (ISO/IEC 24745) • Authentication context for biometrics (ISO/IEC 24761) • Privacy Framework (ISO/IEC 29100) • Privacy Reference Architecture (ISO/IEC 29101) Possible fields of future work documented in the WG 5 Roadmap, include: • in the area of Identity Management, topics such as: - Provisioning - Identifiers - Single sign-on • in the area of Privacy, topics such as: - Privacy impact assessments - Anonymity and credentials - Specific Privacy Enhancing Technologies (PETs) - Privacy Capability Maturity Model

Structure


Abbreviations:
CD – Committee Draft IEC – International Electrotechnical Commission ISO – International Organization for Standardization ITU-T – International Telecommunications Union – Telecommunications Sector JTC – Joint Technical Committee NB – National Body SC – Sub-Committee WD – Working Draft

Conference representation

Observer status granted
May 2009

Observer
Steve Johnston, Office of the Privacy Commissioner of Canada

Meetings attended
4 – 8 May 2009 Beijing, China

Delegate report:

General Comments

The most recent meeting of ISO/IEC JTC1/SC 27/WG 5 was held 4 – 8 May 2009 in Beijing, China.

As with past meetings, progress on current projects was mixed although, overall, more progress was made during this meeting than previously.

Projects

WG 5 is currently working on 9 numbered projects and 2 Standing Documents (SDs). A brief description of the project, as well as a summary of the editing meeting discussions (where attended) for each project, follows:

1) **ISO 24760 – A Framework for Identity Management**. This standard defines and establishes a framework for Identity Management (defined as an integrated concept of processes, policies and technologies that enable organizations and individual entities to facilitate and control the use of identity information in their respective relations). The Framework standard is intended to help designers, architects, evaluators, and users of IT systems building solutions related to identity controls, and to improve adherence to compliance regulations, internal security and privacy policies.

   Progress on this standard has been quite slow. It has been under development for three years and there are still several areas of contention. The vast majority of the comments made on successive drafts of this standard have focused on the following areas:

a) **Terminology**. It has been a major challenge to achieve consensus on the terms and definitions used in this standard, particularly such basic terms as identity, partial identity, identifier and so on. An ad hoc terminology group was created during the Spring 2009 meeting. Using the existing terms and definitions as a starting point, and taking into account comments received from National Bodies (NBs) on the latest version, the group proposed revisions that seem to resolve the terminology issue. There is, however, still the outstanding issue of harmonizing the terms and definitions used in this document with those used by the International Telecommunications – Telecommunications (ITU-T), who are also developing identity management related standards;

b) **Lifecycle**. There is still some debate as to what an identity lifecycle, which is distinct from an identity management lifecycle, should look like. Several different lifecycle models, some based on state transition and others based on process flows, have been incorporated in the standard at one point or another. These models have been merged, separated and modified to the point where none of them are particularly easy to understand. The editors have been tasked with trying to rectify all of the inconsistencies for the next draft;

c) **Structure**. There was still some discussion about the basic structure of the document during the Spring 2009 meeting. A number of changes were made which will be subject to review and comment when the next draft is released.

It was agreed during the Spring 2009 meeting that the document will be informative (should) as opposed to normative (shall) – this was seen to be more appropriate language for a framework, or good practice, standard.

The next version of the document, 1st Committee Draft (CD), is due to be published mid July 2009.

2) **ISO 24761 – Authentication Context for Biometrics**. This standard defines the structure and the data elements of Authentication Context for Biometrics (ACBio), which is used for checking the validity of the result of a biometric verification process executed at a remote site. The specification of ACBio is applicable not only to single modal biometric verification (e.g., fingerprints OR iris scans) but also to multimodal fusion (i.e., combinations of biometrics (e.g., fingerprints AND iris scans)). This standard was published on 15 May 2009.

3) **ISO 24745 – Biometric Template Protection.** This standard is focused on the essential security mechanisms required for the protection of biometric templates.

This document did not progress beyond 2nd Working Draft (WD) for some time. Significant contributions were received, however, during the October 2008 meeting which allowed this document to move forward. Two major issues were resolved during the October meeting:

a) This document will focus on the requirements a biometric template protection solution must/should meet, rather than trying to describe or define specific solutions; and

b) Agreement was reached on what those requirements should be. In that respect, Norway proposed that solutions support renewability and revocability of the biometric templates (possible solutions in this space include cancellable biometrics and biometric encryption). These were seen as desirable properties, not only from a security perspective but also from a privacy perspective.

The inclusion of renewability and revocability generated some debate during the editing session as to whether these should be considered requirements or were actually safeguards or countermeasures. It was eventually agreed that the use of the terms in the text was unclear and inconsistent, so the editor has been tasked to correct this. It was also suggested that the editor consult with SC 37 – Biometrics to see if they have definitions and explanations for these terms that WG 5 should use.

There was some discussion about the potential overlap between this project and ISO 19792 – Security Evaluation of Biometrics. The editor was of the opinion, as were several National Bodies (NBs), that there really wasn't much overlap. The editor agreed, however, to review the document to confirm this.

As with ISO 24760, it was agreed to proceed to the CD stage in hopes that additional NBs will comment. The next version of the document, 1st CD, is due to be published end June 2009.

4) **ISO 29100 – A Privacy Framework**. This standard provides a framework for defining privacy safeguarding requirements as they relate to personally identifiable information (PII) processed by any information and communication system in any jurisdiction. The framework is applicable on an international scale and sets a common privacy terminology, defines privacy principles when processing PII, categorizes privacy features and relates all described privacy aspects to existing security guidelines.

   The framework is intended to serve as a basis for additional privacy standardization initiatives, including a technical reference architecture, the use of specific privacy technologies, assurance of privacy compliance for outsourced data processes, privacy impact assessments and engineering specifications. In order to become widely accepted and to effectively form the basis for additional work, the framework needs to be closely linked to existing security standards that have been widely implemented.

   Progress on this standard has, for the most part, been relatively straightforward. However, the US has expressed concern that this standard was unintentionally setting public policy, which the US considers inappropriate for an ISO standard. This concern is based on the fact that the privacy principles upon which this document is based have not been agreed on a global basis. This issue will be addressed in part by changes made to the language of the document (from "shall" to "should").

In addition, the following should be noted:

a) It is still not entirely clear where the most appropriate place in the standard is to discuss risk management, particularly risks of re-identification (even with supposedly anonymous data), although it was agreed that there should be such a discussion. NBs were asked to carefully consider this issue for the next draft;

b) A clearer distinction is required between a description of a principle (Clause 6) and how to implement it (Clause 7). There also needs to be more clarity with respect to the implementation guidance (e.g., the distinction between having to describe what information will be disclosed, to whom, etc. prior to collection and providing individuals access to a history of disclosures of their personal information (when they exercise their right of individual access) is not entirely clear); and

c) The use of the terms “shall” and “should” within the document was inconsistent. As with the Framework for Identity Management standard, it was agreed that this document would use the term “should”, while supporting standards could use the term “shall”, if appropriate.

The next version of this document, 2nd CD, is due to be published end June 2009.

5) **ISO 29101 – A Privacy Reference Architecture**. This standard is intended to provide a privacy reference architecture model that will describe best practices for a consistent, technical implementation of privacy requirements as they relate to the processing of personally identifiable information (PII) in information and communication systems. It will cover the various stages in data life cycle management and the required privacy functionalities for PII in each stage, as well as describing the roles and responsibilities of all involved parties.

   The privacy reference architecture will present a target architecture and will provide guidance for planning and building system architectures that facilitate the proper handling of PII across system platforms. It will set out the necessary prerequisites to allow the categorization of data and control over specific sets of data within the data lifecycle.

   There was some discussion about including guidance on information classification in the standard. After some discussion, it was agreed that some guidance should be provided for the next draft, and NBs were requested to provide some material from which to work – the US and Korea have already provided some possible material.

   Although the standard is now at 3rd WD, meaning it has been under development for at least 18 months, there are a number of placeholders in the document for which there is still no text due to lack of contributions (e.g., privacy design principles and privacy services).

   The next draft of the document, due to be published in mid July 2009, will be accompanied by a Call for Contributions specifically targeting the architecture components of the standard. If further contributions are not received, it may be necessary to delete certain parts of the document, or perhaps cancel the document outright – neither of these options would be desirable.

6) **ISO 29115 – Entity Authentication Assurance**. This standard is being developed as a common text standard in conjunction with ITU-T Study Group (SG) 17. This standard, currently at 4th WD, provides objective and vendor neutral guidelines for identity assurance. It also describes the guidelines or principles that must be considered in identity assurance and the rationale for why they are important to an authentication decision. The standard provides a framework for assessing "how close" an identity (individual) is to the correct one and provides guidelines for how the strength of the authentication can be measured. It also provides the basis for a set of identity assurance measures that are general and applicable to a wide range of authentication mechanisms.

   The scope of this document has been the subject of considerable debate. Some NBs wanted to restrict the scope so that the document only dealt authentication assurance as it relates to persons, while others wanted it to cover assurance for all types of entities (e.g., persons, devices, applications and so on). It was eventually agreed that the document should be applicable to all types of entities.

There has also been discussion on the relationship between this document and ISO 24760 – there was even a proposal that the two documents be merged. While that proposal was eventually rejected, the links between the two documents will need to be clearly articulated and the respective editors will need to ensure that the two documents are synchronized. There is also a need to clearly determine which part of the identity management framework this document will cover. NBs were asked for contributions in this regard during the next comment period.

The next version of this standard, 5th WD, is due to be published mid July 2009.

7) **ISO 29146 – Framework for Access Management**. This standard is intended to provide a framework for the definition of Access Management and the secure management of the process to access information. This framework would be applicable to any kind of user, individuals as well as organizations of all types and sizes, and should be useful to organizations at any location and regardless of the nature of the activities they are involved in.

   This document is very closely linked to ISO 24760 (Framework for Identity Management) – in many cases, the rationale for performing identity management is to enable access management. For that reason, the editors of ISO 24760 are also the editors of this document. A clear distinction must be made between identity management (who you are, what credentials you hold) and access management (what you are allowed to do).

   Discussions on the 1st WD focused on the scope of the document. It was agreed that this standard should explain the relationship between access management and privacy and security, but not necessarily deal with any associated detail. This standard will not cover specific access control approaches or methodologies (e.g., role-based access control) in any detail, but will provide the framework into which these solutions could fit.

   The next version of this document, 2nd WD, is due to be published mid July 2009.

8) **ISO 29190 - Privacy Capability Maturity Models**. This standard describes a privacy capability maturity model and provides guidance to organizations for assessing how mature they are with respect to their processes for collecting, using, disclosing, retaining and disposing of personal information.

   The study period for this project concluded in October 2008, at which time it was agreed that a New Work Item proposal should be sent to NBs for letter ballot. Having received sufficient support, this item was added to the WG 5 Work Plan.

   One possible outline structure for the document, based on a contribution from the US NB, was presented during the Spring 2009 meeting, along with an explanation of the type of information that should appear in each of the major clauses. This generated some discussion about basic structure, sequencing of the clauses, possible content and so on. The recommendations from the WG included:

   a)Ensure that links to other WG 5 projects are clearly shown, as well as showing how this document might be used (e.g., insert an “applicability” or “application” clause);

   b)The structure of this document should be compared to those of other capability maturity models in order to ensure that no important elements have been missed. A number of possible source documents were mentioned;

c)It was suggested that the title of the document be changed to something like “Privacy Maturity Framework” as the phrase “Capability Maturity Model” has been copyrighted;

d)Consideration should be given to incorporating privacy best practices into the document (e.g., drawing upon the AICPA/CICA Generally Accepted Privacy Principles);

e)Consideration should be given to including an example of an implementation of a maturity model, possibly as Clause 6 or as an informative annex; and

f)Consideration should be given to defining a threshold above which an organization could be deemed to be compliant with relevant privacy and data protection law.

The draft structure of the document will be revised in accordance with the recommendations made during the editing session, including sample text in each of the clauses. This document will then be circulated as part of a Call for Contributions to the text. Contributions are due early August 2009, with a preliminary working draft due by mid September 2009. At the same time, SC 27 will circulate a Call for Editors for this project.

9) **ISO 29191 – Requirements on Relative Anonymity with Identity Escrow – Model for Authentication and Authorization Using Group Signatures**. This standard defines requirements on relative anonymity with identity escrow based on the model of authentication and authorization using group signature techniques. These techniques allow any member of a group to digitally sign a document in a manner such that a verifier can confirm that it came from the group, but cannot determine which individual in the group signed the document. There is usually a group authority of some form that holds the user’s identity in escrow and can reveal that identity under appropriate circumstances. In this way, users can be anonymous to everyone but the group authority.

Development of this standard was proposed by the Japanese NB during the October 2008 meeting. Having received sufficient support, this item was added to the WG 5 Work Plan.

There was only limited discussion of this standard during the Spring 2009 meeting as it is still only a preliminary draft. It was noted that the title of the document will need to be changed to avoid possible confusion with similar projects that are underway in SC 27/WG 2 – Cryptography. A new title – Requirements for Relatively Anonymous Authentication – was proposed. This will need to be approved by NBs as part of the next comment period on this document.

The next version of this document, 1st WD, is due to be published mid July 2009.

10) **SD 1 – WG 5 Roadmap**. The Roadmap provides a visual representation of the possible standards projects that might be undertaken by WG 5, as well as providing some limited sense of the dependencies between the potential projects. The tree structure suggests a hierarchical relationship of the items, when in fact there is a matrix interdependency in many cases (an attempt has been made to show some of these interdependencies via the cross connections in the diagram).

Future versions of the roadmap will look at other options for displaying the information in the diagram, including structuring the activities into a three tier model, dividing them into “strategic”, “tactical”, and “operational” items, or possibly a two tier model using the categories of “What to do” (a management view) and “How to do” (an engineering view).

The Roadmap is updated at every international meeting – the latest version was published immediately following the Spring 2009 meeting.

11) **SD 2 – Official Privacy Documents List**. This document is intended to act as a single reference point for privacy and data protection legislation, regulation, implementation guidelines, codes of conduct and best practice. It is not intended to provide any guidance as to what would be required to achieve and/or demonstrate compliance with any of those laws, etc. – this is to avoid any possible suggestion that this document constituted legal advice.

While it is relatively straightforward to compile this kind of a reference document, keeping it current in the face of legislative changes, issuance of new guidance material and so on may prove to be a challenge. It was agreed that each NB would be responsible for ensuring that their section of the document was current and accurate. The document is to be reviewed at each international meeting.

The next version of this document is due to be published mid July 2009.

Next Meetings

The next WG 5 meetings are scheduled as follows:

- 2 – 6 November 2009, to be held at the Microsoft facilities in Redmond, Washington, USA; and

- 19 – 23 April 2010, to be held in Melaka, Malaysia in conjunction with the SC 27 Plenary (26 – 27 April 2009).

Other Projects of Interest

During the SC 27 Plenary meeting held 11 – 12 May (also in Beijing), several projects were mentioned that might be of interest, including:

a) **ISO 27007 – Guidance for Information Security Management System (ISMS) Auditing**. This International Standard provides guidance on the management of audit programmes, the conduct of internal or external audits of ISMSs, as well as on the competence and evaluation of auditors. It is intended to apply to a broad range of potential users, including auditors, organizations implementing ISMSs, organizations needing to conduct audits of ISMSs, and organizations involved in auditor certification or training, in certification/registration of management systems, in accreditation or in standardization in the area of conformity assessment.

b) **ISO 27008 – Auditing of Information Security Controls** (more technical in nature than ISO 27007). This Technical Report provides guidance for assessing the implementation of ISMS controls selected through a risk-based approach (e.g., as presented in a statement of applicability) for information security management. It supports the information security risk management process and assessment of ISMS controls by explaining the relationship between the ISMS and its supporting controls. It provides guidance on how to verify the extent to which required ISMS controls are implemented. Furthermore, it supports any organization using an ISMS to satisfy assurance requirements, and as a strategic platform for Information Security Governance. This technical report is applicable to all organizations,

including public and private companies, government entities, and not-for-profit organizations. This document is applicable to organizations of all sizes regardless of the extent of their reliance on information.

c) **ISO 27036 – Guidelines for the Security of Outsourcing**. This International Standard will define guidance to organizations on the evaluation of security risks involved in the procurement and use of outsourced services. This standard will support the implementation of ISO/IEC 27001/27002 controls for outsourcing and should include the following areas:

1) Strategic goals, objectives and business needs;

2) Risks and mitigation techniques; and

3) Assurance provision.

Note: It is the intent of this standard that outsourcing is not limited to ICT outsourcing, but could include other forms of outsourcing (e.g. human resources, facilities management) that have information security implications.

The 1st WD of this standard is to be published by end June 2009.

d) **ISO 27037 – Guidelines for the Identification, Collection and/or Acquisition and Preservation of Digital Evidence**. This International Standard will provide guidance concerning identification, collection and/or acquisition, marking, storage, transport, and preservation of digital evidence. This standard will cover acquisition of digital evidence from various types of sources including, but not limited to:

1) static data sources;

2) data in transit (e.g. over networks); and

3) volatile data sources (e.g. mobile phones).

The scope uses the term “digital evidence” to mean information that meets the requirements of the relevant jurisdiction for use in legal proceedings. As the standard is developed, care will be taken to use terminology that is not limited to a particular jurisdiction or purpose. The scope does not include matters pertaining to analysis of digital evidence, or admissibility, weight, relevance, and other judicially-controlled limitations on the use of digital evidence in courts of law. The proposed international standard will not mandate the use of particular tools or methods.

The 1st WD of this standard is due to be published by end June 2009.

e) **JTC 1 Study Period on Digital Content Management and Protection**. There is very little information available about this study period at the moment, but based on the title, this may have something to do with technical protective measures (for the protection and enforcement of copyright). The initial meeting of the Study Group is scheduled for 15 – 17 July 2009 in Beijing, China;

f) **WG 4 Study Period on Redaction**. A new project proposal was submitted by the UK on the topic of redaction, which is the procedure for removing sensitive or classified information from documents (electronic or otherwise) to be released publicly. SC 27/WG 4 agreed to

initiate a Call for Contribution for a rapporteur and contents for a new study period on this topic. The Call for Contribution is to be issued by 30 June 2009; and

g) **SC 27 Vocabulary Harmonization**. There was also a proposal from Canada to create an ad hoc study group on the harmonization of terminology within SC 27. While there was general agreement in principle for such an activity, several NBs expressed reservations over the creation of yet another group that would consume scarce resources. An ad hoc group was established to develop a proposal for a process for terminology harmonization. The group is comprised of representatives from Poland, New Zealand, Germany, Canada and the UK – Canada is to provide the Rapporteur for the group.

ISO TMB Task Force on Privacy

In June 2008, ISO's Technical Management Board (TMB), the most senior management body within ISO, established a Privacy Task Force (TF) to "explore and advise the TMB on ISO technical standards that can support the implementation of public policy initiatives on Privacy, with specific focus on protection of personally identifiable information (PII) and fair information handling." In chartering the TF, the TMB directed that the TF identify the variety of public policy on this topic and make an inventory of existing standards from ISO, IEC and other sources noting how they currently support such public policy. The TMB noted that the TF shall not recommend ISO standards whose content can be perceived to assume the roles of public policy making parties or that seek to drive public policy agendas.

The membership of the TF was based on one nomination from each TMB member[7]. The TF met once, in December 2008 in Berlin, at which time it agreed to undertake a survey of various ISO and other Technical Committees (TCs) that deal with some aspect of privacy in their work programmes. The TF invited input on current and future work programs, the need for assistance or guidance from the TMB, and suggestions for further ISO standards activities.

The TF has now completed its deliberations and has submitted its final report for consideration at the upcoming TMB meeting, to be held 14 September 2009. The TF made a number of key recommendations, including:

1) ISO should consider leading an effort to engage the broader standards community now working on privacy to intensify their interaction. Although various groups consulted appear to be delivering what is needed to their immediate constituencies; however much work still needs to be done to share relevant information and to better coordinate the work being done by the various stakeholders working on standardization in the area of privacy. An important first step could be the holding of a conference between all involved committees. The aim of such a conference would be to prepare a global inventory of privacy-related standards work and develop some form of overarching roadmap which defines a strategic vision for the standards development work in this area;

2) There is strong desire to establish a common terminology document in the area of privacy and privacy principles. Individual committees have developed similar parallel solutions to address the situations peculiar to their topic. There has been a notable degree of collaboration leading to much common use of standards materials, however,

[7] The TMB is composed of one representative from each of the 12 elected member bodies of Brazil, Canada, China, France, Germany, Japan, Netherlands, Norway, Spain, South Africa, the UK and the US. Michel Bourassa (Director, Standards, SCC) is both Canada's representative to TMB and the Convenor for the new TF.

there are still differences in how various terms are used and understood. These differences could be reduced or eliminated through the establishment of a horizontal common terminology document. ISO is to consider ways in which to establish such a document; and

3) It is recommended that ISO establish a "live" inventory (i.e., document and/or dedicated webpage) for its TCs that would encourage sharing of information for ongoing privacy related work;

4) To ensure continued relevance of ISO's standardization work related to privacy, it is essential to engage with public policy organizations and to initiate dialogue on commonality. ISO may want to focus on collaboration with key stakeholders at the policy and technical level such as the International Conference of Data Protection and Privacy Commissioners, OECD, CEN and member countries' Data Protection Authorities (DPAs) to examine the level of commonality on accepted privacy principles. It may also wish to investigate the development of a mechanism to provide guidance on developing privacy standards to complement regulation;

5) ISO should continue in its efforts to identify and work with key stakeholders, analyzing work streams and standards work that could support the development of an international privacy standard and continue to identify, map and coordinate the various (ISO) privacy work streams to help deliver consistency in language, objectives etc, and to ensure that standards can be adopted, deployed and measured by organizations in a systematic and effective manner.

TMB will render a decision on the draft TF report through the adoption of a resolution. An advance copy of the proposed resolution, which may or may not be adopted as drafted, states that TMB:

a) Decides that a Privacy Steering Committee shall be **created reporting to the TMB** with a view to: 1) implementing the three (3) Task Force recommendations and 2) assessing the feasibility of implementing the three (3) additional recommendations;

b) **Assigns the secretariat of the Privacy Steering Committee to JTC 1/SC 27**;

c) Requests the Central Secretariat to issue to TMB members a call for the nomination of experts and the secretariat of the Privacy Steering Committee to invite other committees and working groups within ISO that have worked on privacy-related standards to join the Privacy Steering Committee; and

d) Further requests the Privacy Steering Committee to provide the following to the TMB for approval at its June 2010 meeting: 1) an outline of its proposed workplan and related timeframes, and 2) a list of the members of the Privacy Steering Committee, including the ISO committees and the experts nominated by TMB.

Annex H:

Steering Group resolution

The Steering Group proposes the following resolution:

Directions to Steering Group to consider seeking observer representation before Internet Governance Forum, London Action Plan and ICANN

The 31st International Conference of Data Protection and Privacy Commissioners:

1. **Notes** that the Steering Group on Representation before International Organisations has, in accordance with directions given by the 30th Conference, sought or obtained observer representation before the appropriate committees or working groups of APEC, Council of Europe, ISO and OECD;

2. **Further notes** that while the Steering Group has not considered it appropriate to seek representation before the International Law Commission, International Telecommunications Union and UNESCO at this stage that it plans to continue to explore the usefulness of seeking representation at a future date; and

3. **Now directs** the Steering Group to explore the usefulness of obtaining observer representation, and if appropriate to obtain observer representation from the following:
   (a) Internet Governance Forum;
   (b) London Action Plan (on spam); and
   (c) Internet Corporation for Assigned Names and Numbers (ICANN).

Explanatory note

The Steering Group has reviewed the international scene and recommends that the Conference give it additional directions to seek observer status, if warranted, from three further international bodies.

The Internet Governance Forum (IGF) was established to support the United Nations Secretary-General in carrying out the mandate from the World Summit on the Information Society (WSIS) for multi-stakeholder policy dialogue. The IGF facilitates discussion on Internet governance issues through that website, workshops and through an annual meeting (in 2009 to be held in Egypt). Being an observer to this forum would give a higher visibility to data protection issues and enhance engagement with elements interested in Internet issues.

The London Action Plan, a joint initiative of several international organisations. This is a group of enforcement authorities that aim to coordinate action in relation to spam. Several data protection authorities already participate in this forum.

ICANN describes itself as a 'not-for-profit public benefit corporation with participants from all over the world dedicated to keeping the Internet secure, stable and interoperable'. It develops policy on the Internet's unique identifiers.

These forums are less formal than traditional international governmental organisations. However, that does not mean that they are unimportant. In the challenging area of Internet regulation and enforcement, it may be that new means of innovative cooperation in standard setting and enforcement are needed.

While the Steering Group has identified these groups as of potential interest to the Conference it has not completed a detailed evaluation. The direction sought in the resolution will provide a basis for the Steering Group to take the matter further. Further examination of the bodies' work plans for 2010 and beyond will assist in determining whether engagement as an observer will offer value to all parties. The Steering Group will also examine logistical issues including whether there are DPAs available to be the Conference's delegates.

Annex I:

Second Steering Group Resolution: Admitting International Observers to the Conference

The Steering Group proposes the following resolution:

Admitting Observers from International Governmental Organisations to the Closed Session of the Conference

That the 31st International Conference of Data Protection and Privacy Commissioners adopts the following policy for admitting observers from international governmental organisations to the closed session of the Conference:

1. The Conference approves the international governmental organisations listed in the schedule as initial observers for a period of three years. The listed organisations may apply for a continuation of their observer status in accordance with the process established by this resolution.
2. Any international governmental organisation may apply to the Steering Group on Representation before International Organisations to be admitted as an observer. The Steering Group may grant observer status either for a particular Conference or for any period not exceeding three years.
3. International governmental organisations should apply in writing at least two months before the Conference. Approved observers will be admitted to the closed session by the host of the Conference. Late applications may be accepted in the discretion of the Steering Group. However, in the case of approvals granted on late applications, hosts may refuse entry to the closed session if there is insufficient space available.
4. Admission of approved observers to the closed session is subject to the observer having:
   (a) registered for the Conference;
   (b) met any administrative requirements imposed by the host (such as completing a form or paying applicable fees).

Annex of initial observers

Organisation for Economic Cooperation and Development (OECD)
Council of Europe

Explanatory Note

The Conference has for many years admitted observers from selected international organisations in the closed session. The 29th Conference resolved that it would revisit the issue of admitting observers from international governmental organisations in due course with a view to adopting a standard list of approved observers for the convenience of hosts and governmental international organisations.[8] This resolution establishes a new more transparent process that will provide greater certainty to international organisations that wish to observe the proceedings of the Conference.

[8] Resolution on Conference Organisational Arrangements, clause C, Montreal, 2007.

This resolution approves an initial group of international governmental organisations as observers to the Conference. The resolution also establishes a process for other international governmental organisations to obtain observer status and for the listed organisations to continue their observer status after of the initial three years. The role of granting observer status for international governmental organisations transfers under this resolution from the Conference host to the Steering Group on Representation before International Organisations.