TECHNICAL MANAGEMENT BOARD PRIVACY TASK FORCE

FINAL REPORT SEPTMBER 2009

PREAMBLE

This report provides:

- Introduction (History and background on the Privacy TF work)
- Results of the consultations (Overview of the TF Inventory and ISO/IEC/JTC1/SC27/WG5)
- 3 consensus recommendations (Task Force Recommendations)
- 3 other recommendations (Additional Recommendations)

At the end, the TMB is requested to consider the report, to decide whether ISO should pursue the topic, and if yes, provide direction.

INTRODUCTION

The Technical Management Board (TMB) established a Privacy Task Force (TF) in June 2008 to explore and advise 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 may 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 impetus behind this initiative is the rapidly changing nature of how individuals provide private information for access to many services (both private and public) and what is made of that information. Citizens and consumers today have never before led such data rich lives, detailed data footprints are continually created, left and re-shaped during the lifetime of an individual's engagement with private and state organisations. Technological developments, increased electronic capture and sharing of personal information, combined with the internationalised nature of data processing, has led to calls to assess the adequacy of and need for international privacy standards. This demand is driven by privacy advocates and some members of the international data protection regulatory community who continue to voice a desire to see the development of international privacy standards that meet the expectations and demands of individuals and that support national laws and other privacy instruments across global operations. It is also driven in part by businesses seeking consistency in establishing and implementing technical solutions, architectures and privacy management practices and processes that can be applied across their global operations to provide for effective privacy controls over the information which is gathered consistent with applicable laws and regulations. The challenge when it comes to standardization is that there are multiple privacy instruments (i.e., legislation, regulations, guidelines) around the world. This multiplicity of privacy instruments that currently exist aim to achieve the same goals and they are, to a large extent, built upon the same fundamental principles; however, some countries use an omnibus horizontal legislative approach to protect PII while others rely on a range of measures including federal and state laws and regulations, voluntary codes, seal programs, corporate and government policies, court decisions, treaties, inter-governmental agreements, standards and contracts. The challenge of finding a common set of principles that can accommodate this diversity is not insurmountable.

OVERVIEW OF THE TASK FORCE INVENTORY

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.

Fourteen responses were received and analyzed by the TF (See Annex A /TF N05). The responses provide a useful inventory of the current, future and in some cases, past work that the respondents are engaged in relating to privacy, PII and fair information handling.

The responses left little doubt that there is a significant amount of privacy-related work being done within the ISO system and among the non-ISO groups consulted. Though some of the standards (or tools, guidance, TR, etc.) have broader application, the committees and groups consulted seem to be addressing issues related to privacy as they arise within the context of their particular areas of responsibility, and more specifically, within the context of specific subjects or topics. Respondents drew attention to the complex web of legal and regulatory (i.e. non-voluntary) frameworks relating to privacy, PII and fair information handling, reflecting the inherent challenge of striking a balance between the voluntary international standards and mandatory national legal frameworks.

As would be expected, the responses reflect the diverse and complex nature of privacy, PII and fair information handling. Inherent in the responses is recognition of the challenges associated with finding a universal approach. This was most evident in the two responses that asserted that no guidance could be practically provided by the TMB due to the unique nature of privacy. However, the requests for a detailed global inventory or mapping and a mechanism for coordination and information sharing also reflect the enormity and complexity of the subject. There is currently no one single source that provides a global overview of the complex web of laws, regulations, standards, instruments, tools, guidance, etc. regarding privacy, PII or information handling in the various areas in which the issue arises.

Ten of the fourteen respondents did not provide any suggestions for further standards activities to support the implementation of public policy initiatives on data privacy, PII or fair information handling that could complement existing national or international standards. This could be interpreted to suggest that the current approach of addressing privacy-related issues in the context of specific subjects is adequate. Indeed, respondents expressed concerns that added standardization could complicate rather than help matters.

Suggestions for future standardization activities were submitted by four respondents, which can be grouped in the following five categories: a) definitions for privacy-related terminology; b) respect for the privacy of persons with disabilities; c) clarification of the scope of privacy-related activities; d) standards related to privacy and individuals; and e) an invitation for suggestions regarding Health Informatics.

Regarding the five suggestions for further standardization activities made by four respondents, the answers to Question 1 provided by all respondents suggest that many of these activities are already, to some extent, currently addressed within the scope and mandate of individual committees. If a more universally applicable approach is needed, a mechanism could be created to improve the coordination between committees (and groups) whose mandates have led them to address various aspects of privacy, PII or fair information handling in standards or various instruments. A meeting of these committees (and groups) may be a useful starting point in this

regard specifically when committees or groups respond when they identify areas that they think need to be addressed but which fall outside of their current mandate. Processes need to be developed so that these issues can be addressed and decisions made.

ISO/IEC JTC1/SC27/WG5

Notable in the survey responses was the extensive work being done in ISO/IEC JTC1/SC 27/WG 5 on Identity Management and Privacy Technologies. Work items include:

- ISO/IEC 29100 (CD), *Information technology -- Security techniques -- A privacy framework* provides a framework for defining privacy safeguarding requirements as they relate to PII processed by any information and communication system in any jurisdiction.

- ISO/IEC 29101 (WD), *Information technology -- Security techniques -- A privacy reference architecture* 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.

- ISO/IEC 29190 (WD), *Information technology -- Security techniques -- A Privacy Capability Maturity Model* 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.

WG 5 also has developed Standing Document 1, a roadmap of existing projects, work items, and activities of WG 5, as well as possible fields of future work.

The membership of WG 5 includes recognized privacy experts from multiple commercial vendors and providers of IT products and services, as well as government officials, third-party auditing firms, and academics from different countries.

Significantly, WG 5 also maintains two-way liaison with the International Conference of Data Protection and Privacy Commissioners (ICDPPC).[1] The ICDPPC will consider at its 31st conference in November 2009 a resolution calling for a "Joint Proposal for Setting International Standards on Privacy and Personal Data Protection" that would be a "universal legally binding instrument."[2] It should however be noted that in the context of this proposal the term standard does not refer to technical standards but rather models or examples in the sense of the current Merriam-Webster Online Dictionary[3]

To the extent there is a "focal point" on privacy work within ISO at the technical level and in terms of engagement with public policy organizations dealing with this issue, WG 5 is it. Keeping any future work on privacy in WG5 will ensure that it is coordinated with existing security standards work under SC27. It should however be noted that the decision to assign responsibility for privacy related work in SC 27 was not without controversy. One of the recommendations that came out of

[1] The ICDPPC accepts membership based on the existence of an independent privacy enforcement body akin to a data protection authority. Countries which do not have such a centralized data protection authority, the U.S. for example, have observer status in the ICDPPC and no voting rights.
[2] See http://www.privacyconference2009.org/privacyconf2009/dpas_space/index-iden-idweb.html
[3] "Something set up and established by authority as a rule for the measure of quantity, weight, extent, value, or quality", from http://www.merriam-webster.com/dictionary/standard

the Privacy Technology Study Group in 2004 was the creation of a separate SC for Privacy which still has not been created. The Terms of Reference for WG 5 focus on security aspects of identify management, biometrics, and the protection of personal data which are only part of the privacy spectrum.

TASK FORCE RECOMMENDATIONS

The Analysis of Questionnaire Responses conducted by the TF as well as TF member comments suggest a desire for 1) greater information sharing and coordination among committees engaged in privacy work, 2) a common terminology document, and 3) a live public inventory of privacy initiatives. The TF requests that the TMB consider the following recommendations.

1) ISO should consider leading an effort to engage the broader standards community now working on privacy to intensify their interaction. From the work conducted it appears that various groups consulted are 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 (see #3 below). It would also help to revitalize existing liaisons between committees, identify new liaisons that might need to be established and perhaps provide a mechanism for ensuring more complete and timely exchange of information to reduce confusion, minimize conflicting standards and foster engagement and common understanding.

In order to maximize output it is recommended that such a conference not be fully open to the public. Rather ISO should issue invitations covering the Chair and possibly one or two additional representatives from those committees involved as well as inviting other key stakeholders such as CEN, the International Security, Trust and Privacy Alliance (ISTPA), and the International Conference of Data Protection and Privacy Commissioners.

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, there are 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. Recognizing that standardizing terminology in the area of privacy is challenging, the TMB may find it preferable to make use of existing documents, expertise and established procedures. ISO may wish to:

- Consult with JTC 1/SC 27 on further developing their Standing Document 6, Glossary of IT Security Terminology, which is publicly available,
- Further consult with the International Security, Trust and Privacy Alliance (ISTPA) and their *Analysis of Privacy Principles: Making Privacy Operational*,[4] an earlier effort to analyze multiple privacy instruments around the world and derive composite and harmonized definitions for fourteen privacy requirements that are most commonly in use today

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

[4] See http://www.istpa.org/pdfs/ISTPAAnalysisofPrivacyPrinciplesV2.pdf

work. Use should be made of existing documents such as Standing Document 2 of JTC 1/SC 27/WG 5 (Official Privacy Documents Reference List) and the inventory and questionnaire analysis that was compiled by the TF in carrying out its activities. With such a live mechanism, TCs should be encouraged to add and record new developments as they occur. These measures would also encourage and strengthen appropriate liaisons between TCs and assist in coordination efforts. Maintenance should be assigned to ISO or to a specific ISO TC (e.g., JTC1/SC 27/WG5) and be kept live on the ISO website.

ADDITIONAL RECOMMENDATIONS

Several additional recommendations were suggested by TF members. Unanimity on these recommendations was not achieved. These include recommendations to actively engage with public policy organizations and further investigation of the value of an ISO standard which sets out basic privacy principles.

4) Given the rapid IT evolution there are many innovative ways to use and manage information. In keeping with this tremendous pace, public policy too is evolving but at different rates in different jurisdictions. 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. This dialogue is necessary if ISO is to live up to its ambit of providing useful tools and concepts to assist the implementation of public policy as it evolves. It will be useful for ISO to find the proper balance between what ISO can do to support the implementation of evolving public policy while not forcing public policy through standards development. 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) Although it has been suggested that the complexity of national and international data protection and privacy laws makes it impossible to develop an ISO privacy standard, especially one of a management nature, there are common principles running through the various national and international laws that could enable the development of an ISO privacy standard. An ISO privacy standard is increasingly needed in the ever developing networked and distributed computing and communications environment which is shaping and determining the privacy of personal information and communications, and which transcends political boundaries.

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.

6) A common framework of fundamental privacy standards is considered desirable, on which sector related work can and should be built. A significant portion of such a framework is already available or under way within the work programme of JTC 1/SC 27/WG 5. Using the network of liaisons, JTC 1/SC 27/WG 5 could be systematically informed about sector specific needs in order to address them in its own work programme. As a starting point WG 5 should make its roadmap document widely available. This would identify for others the work that is ongoing in WG 5, identify standards that should be developed, and it would allow other stakeholders to identify where their existing standards fit into the overall structure and it would provide an opportunity to

suggest changes to the structure. The resulting compilation could form the basis for an ISO level framework.

TECHNICAL MANGEMENT BOARD ACTION: The TMB is invited to

a) accept the report
b) consider the recommendations
c) disband the Task Force