Commissioners call for an International Privacy Convention

Saira Ahmed and Prashanti Ravindra[1]
Galexia[2]

This paper is available in the following formats from <http://consult.galexia.com/>:

- HTML[3]
- PDF[4]

Contents

[1] Saira Ahmed and Prashanti Ravindra are Research Consultants at Galexia where they undertake legal research on privacy and e-commerce issues in Australia and Asia.

[2] <http://www.galexia.com>.

[3] HTML version of paper: <http://consult.galexia.com/public/research/articles/research_articles-art36.html>.

[4] PDF version of paper: <http://consult.galexia.com/public/research/assets/calls_for_un_privacy_convention_200511.pdf>.

1. Introduction

Privacy commissioners around the world have called for the United Nations to prepare a convention on data protection. The proposed convention will recognise the universal nature of data protection and privacy rights and will seek to overcome the inconsistencies and barriers to cross-border information exchanges created by inconsistent data protection regimes.

The proposals for a universal privacy convention were made following the 27th International Conference of Data Protection and Privacy Commissioners (Montreux, Switzerland, 14-16 September 2005)[5]. The Conference was attended by privacy and data protection commissioners from over 40 countries and more than 300 participants from business, public administration, the IT industry and government and non-government organisations who attended the open-sessions at the conference.

In addition to the need for international mechanisms to protect personal data, other conference themes included privacy challenges in clinical research, privacy protection in the face of terrorism, privacy challenges arising from biobanks and the importance of self-regulation in implementing data protection principles.

As well as the Montreux Declaration calling for the protection of data in a globalised world[6] the Conference yielded two resolutions adopted by the data protection and privacy commissioners gathered at the conference.[7] A resolution on the use of biometrics in passports and the need for effective safeguards and technical restrictions to control the use of biometric data in passports and identity cards was adopted. As was a second resolution on the use of personal data for political communication that recognised the need for data protection principles such as data minimisation and lawful collection to be maintained when processing personal data in the course of a making a political communication.[8]

The Montreux Declaration recognises the increasing cross-border context surrounding data exchange; the disparity in national and regional data protection regimes; and the protection of privacy as a fundamental human right and recommended the creation of a convention to strengthen the universal character of data protection principles.

This article includes detailed information about the Declaration and the proposal for an international convention. This article also considers other international and regional efforts aimed at promoting harmonisation of privacy laws and the potential impact of a UN data protection privacy convention.

---

[5] <http://www.privacyconference2005.org/>.

[6] *Montreux Declaration – The protection of data and privacy in a globalised world: a universal right respecting diversities*, 27th International Conference of Data Protection and Privacy Commissioners, 14-16 September 2005, Montreux, <http://www.privacyconference2005.org/fileadmin/PDF/montreux_declaration_e.pdf>.

[7] *Resolution on the use of biometrics in passports, identity cards and travel documents*, 27th International Conference of Data Protection and Privacy Commissioners, 16 September 2005, <http://www.privacyconference2005.org/fileadmin/PDF/biometrie_resolution_e.pdf>; and *Resolution on the Use of Personal Data for Political Communication*, 27th International Conference of Data Protection and Privacy Commissioners, 14-16 September 2005, <http://www.privacyconference2005.org/fileadmin/PDF/political_communication_resolution_italy_e.pdf>.

[8] This resolution was presented by the Italian delegates.

2. Montreux Declaration

Recognising the volatile environment created by the emergence of information technologies coupled with the globalisation of information exchange, privacy commissioners from around the world have taken initial steps towards resolving concerns over the protection of personal data. The Montreux Declaration builds on progress made at previous Conferences[9] and is aimed at harmonising the worldwide disparity in approaches to privacy legislation.

The Declaration calls for three initiatives designed to strengthen the universal nature of data protection principles:

> 1. The United Nations to prepare a legally binding instrument which affirms data protection and privacy as enforceable human rights.
>
> 2. Governments around the world to enact privacy and data protection legislation in line with recognised data protection principles and to extend it to their mutual relations.
>
> 3. The Council of Europe to invite non-member states to accede to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data.

To further these aims, the commissioners appealed for international and supra-national organisations to commit themselves to complying with data protection principles consistent with international legal instruments, international non-governmental organisations to develop data protection standards and hardware and software manufacturers to develop products and systems integrating privacy-enhancing technologies.

The Commissioners pledged their support to the realisation of these initiatives through greater collaboration with governments, international and supra-national organisations with a view to adopting a universal convention on data protection.

Progress in achieving these objectives will be regularly monitored, with the first assessment to take place at the 28th International Conference in 2006 (in Argentina).

[9] *Venice Declaration*, 22nd International Conference of Data Protection and Privacy Commissioners, 28-30 September 2000, Venice, <http://www.privacyconference2003.org/pdf/Venice_Declaration.doc>. *Resolution on Data Protection and International Organisations*, 25th International Conference of Data Protection and Privacy Commissioners, 10-12 September 2003, Sydney, <http://www.privacy.gov.au/news/resint.html>.

3. Other International Privacy Instruments

The Montreux Declaration can be viewed as one of a number of international and regional efforts to promote an internationally harmonised privacy law. The creation of an UN privacy convention would serve to crystallise these efforts and forge a body of unified global data protection principles. Existing multi-national data protection legal initiatives, both binding and non-binding will inevitably shape the form a privacy convention may take. Some of these are briefly discussed below.

3.1. EU Data Protection Directive

Data protection legislation in the European Union (EU) has been harmonised through member country implementation of the EU Data Protection Directive (95/46/EC).[10] The harmonisation of data protection laws as facilitated by the Directive is intended to improve cross-border data flows by removing obstacles to transborder information exchanges while maintaining a high standard of information privacy in the EU. The Directive affords all citizens an equal standard of data protection across the EU.

The Directive contains a number of provisions on the processing of personal information and the rights of data subject's over their personal information. Principles of data protection embodied in the Convention include that data must be processed lawfully and fairly, data collected must be relevant for the purpose it was collected, data must be kept accurate and data controllers must provide reasonable measures for data subjects to rectify, erase or block access to incorrect data about them.

Subject to some exceptions, transfer of personal data for processing to countries outside the EU is only allowed under the Directive where an adequate level of protection can be guaranteed. This is to be assessed by reference to, inter alia, the circumstances surrounding the data transfer, the nature of the information and the data protection laws in the third country[11]. This provision ensures that data protection standards are maintained in data transfers outside the Union.

The mechanism for recognition of countries that provide adequate, and more importantly inadequate protection under the Directive could be difficult to translate to an international stage. This would be the case if the provision were to be adapted for an international privacy convention. The Directive requires member states and the European Commission to inform each other if they consider a member country does not offer an adequate level of protection.[12] The provision is necessary to help ensure that the data protection standards in the Directive are maintained. It would be prudent if an international privacy convention were created that it contained a similar provision. This could perhaps be achieved by a register maintained by the UN agency responsible for drafting the Convention of countries that do not provide adequate standards of information privacy.

[10] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, <http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm>.

[11] Article 25.

[12] Ibid.

There may be difficulty in acquiring sufficient consensus for a formal process of recognising countries that do not offer adequate data protections. In addition to political complexities and sensitivities, such a process would have high administrative overheads. A better and more feasible alternative would be to maintain a register of countries who had implemented the convention. A similar practice of noting countries who have signed or acceded to any given UN convention already occurs.

3.2. Safe Harbour

The Safe Harbour framework has been created by the United States' Department of Commerce and the European Commission in an effort to reconcile the differing approaches to data protection in the United States and the EU. The United States uses a sectoral approach that relies on a combination of legislation, regulation and self-regulation. The EU, as discussed above, uses comprehensive legislation to control the processing of personal data.

The Safe Harbour framework, approved by the EU in July 2000[13], is essentially a certification scheme for US companies to satisfy the 'adequacy' provisions of the EU Data Protection Directive. The Safe Harbour framework is based on seven principles:

- Notice;
- Choice;
- Onward Transfer;
- Access;
- Security;
- Data integrity; and
- Enforcement.[14]

Certification under Safe Harbour ensures that data transfers to a US company from any EU member states will be permitted. It removes fetters American companies may face in their trans-Atlantic transactions and the possibility of prosecution by European authorities for failing to comply with the EU's data protection laws. The framework is essentially a compromise reached between the EU and the United States to address the differing approaches to data protection.

A 2004 implementation study prepared for the European Commission found that efforts made by American organisations to comply with the Safe Harbour framework do not necessarily ensure adequate safeguards for personal data.[15] According to the Study, US organisations seemed to have difficulty translating the framework into their data protection policies. This was due to a lack of understanding about their obligations under Safe Harbour and possibly a discordant perception of what personal data protection involves.[16] The study emphasises the practical difficulties in ensuring adequate processing of personal information and that more is needed than simply regulatory measures or bilateral agreement.

---

[13] <http://europa.eu.int/comm/justice_home/fsj/privacy/law/index_en.htm>

[14] See: US Department of Commerce, *Safe Harbour Overview*, Website, Accessed 9 November 2005, <http://www.export.gov/safeharbor/sh_overview.html>.

[15] Asinari, Dhont and Poullet, *Safe harbour Decision Implementation Study,* 19 April 2004, <http://europa.eu.int/comm/justice_home/fsj/privacy/docs/studies/safe-harbour-2004_en.pdf>, p 105.

[16] Ibid.

3.3. OECD Guidelines

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data[17] were adopted on 23 September 1980 as a Recommendation of the Council of the OECD to provide a framework for harmonising national data protection laws amongst member countries.[18] These Guidelines aim to remove obstacles to the transborder flow of information brought about by disparities in domestic legislation.

The OECD Guidelines encompass eight 'Basic Principles of National Application' concerning the collection, storage, and management of personal information:

> 1. Collection Limitation Principle – Collection of personal data should be limited, data should be obtained lawfully and fairly and, where appropriate, with the knowledge or consent of the data subject.
>
> 2. Data Quality Principle – Personal data should be relevant to the purposes of intended usage and should be accurate, complete and up-to-date.
>
> 3. Purpose Specification Principle – The purposes for which personal data is collected should be specified at the time of data collection and subsequent use limited to this purpose.
>
> 4. Use Limitation Principle – Personal data should not be disclosed, made available or used for purposes other than those specified in accordance with [Principle 3] except with the consent of the data subject or by the authority of law.
>
> 5. Security Safeguards Principle – Personal data should be protected by reasonable safeguards.
>
> 6. Openness Principle – There should be a general policy of openness about developments, practices and policies surrounding personal data.
>
> 7. Individual Participation Principle – Individuals have the right to inquire, be given access to and challenge personal data held by the data controller and have this data erased, rectified, completed or amended if the challenge is successful.
>
> 8. Accountability Principle – The data controller shall be accountable for compliance with data protection rules.

Interestingly at the time the Guidelines were released, it was foreseen that "the Guidelines could serve as a starting-point for the development of an international convention when the need arises."[19] The explanatory note to the Guidelines states that except where expressly provided[20], application of the Guidelines is not limited only to relationships between member countries.[21] Further, it is noted that efforts shall be made to raise awareness of the Guidelines amongst non-member countries.

---

[17] OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Paris, 1980, <http://www1.oecd.org/publications/e-book/9302011E.PDF>.

[18] The OECD member countries are: Australia, Austria, Belgium, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

[19] Paragraph 30, OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Explanatory Note*, Paris, 1980, <http://www1.oecd.org/publications/e-book/9302011E.PDF>.

[20] ss 15, 17 and 20, OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* Paris, 1980, <http://www1.oecd.org/publications/e-book/9302011E.PDF>.

[21] Paragraph 28, OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data – Explanatory Note*, Paris, 1980, <http://www1.oecd.org/publications/e-book/9302011E.PDF>.

The Guidelines were a considerable development at the time they were announced and represented international consensus on fundamental principles of privacy and data protection. There is criticism[22] however that the Guidelines are considerably general and as such fail to adequately address the intricacies of information privacy that have resulted from recent technological advances. The Guidelines could serve as a starting point for coordinating an international approach but would need to be updated in light of today's online environment.

3.4. APEC Privacy Framework

The APEC Privacy Framework[23] was created by the Asia Pacific Economic Cooperation in November 2004 in response to a proposal from Australia to develop an Asia-Pacific privacy standard for its 21 member economies.[24] The Framework contains nine Privacy Principles (Preventing Harm; Notice; Collection Limitation; Uses of Personal Information; Choice; Integrity of Personal Information; Security Safeguards; Access and Correction; and Accountability) largely reflecting those contained in the OECD Guidelines. An additional principle "preventing harm" is included, which recognises the harm that may result from the misuse of personal information and the need for remedies addressing this harm to be proportionate to the likelihood and severity of the harm.

The APEC Privacy Framework has been met with substantial criticism. Privacy groups argue that it fails to completely implement the principles embodied in the OECD Guidelines and further, it fails to address the shortcomings of these twenty five year old Guidelines.[25] If the APEC Framework were to be utilised in the development of an international convention, clearly these shortfalls would need to be addressed.

3.5. ISO Personal Information Protection Standard

In the late 1990's the International Standards Organisation (ISO) considered the idea of developing an international standard for the protection of personal information[26]. An Ad Hoc Advisory Group (AHAG) was established to consider the desirability and practicability of the ISO developing an international data protection standard.

However, the AHAG meetings never resolved the key question of what form the standard should ultimately take. Possible forms of an ISO instrument included a set of principles, a management standard and a technical standard.

---

[22] Clarke, R, *Beyond the OECD Guidelines: Privacy Protection for the 21st Century*, 2000, <http://www.privacy.gov.au/act/review/Att5-PP21C.pdf>.

[23] Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, Nov. 2004, <http://203.127.220.112/content/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.downloadlinks.0001.LinkURL.Download.ver5.1.9>.

[24] The APEC member economies are: Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Republic of the Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; United States of America and Viet Nam.

[25] See for example, Australian Privacy Foundation, *Submission to the APEC Electronic Commerce Steering Group Privacy Sub-Group – Recommendations for Improvements to APEC Privacy Principles (Version 9)*, 19 March 2004, <http://www.privacy.org.au/Papers/APEC0403.html> and Asia-Pacific Privacy Charter Council, *Submission to the APEC Electronic Commerce Steering Group Privacy Sub-Group – Submission concerning the APEC Privacy Principles (Consultation Draft)*, <http://www.bakercyberlawcentre.org/appcc/APEC_APPCCsub.htm>.

[26] Connolly, Chris, *An international standard for privacy* [1997] PLPR 48 <http://www.austlii.edu.au/au/journals/PLPR/index.html>

Another important consideration was the relationship between an ISO instrument and the EU Data Protection Directive. While a definitive position was never formed by AHAG, it would be difficult for the standard to claim it was an 'international' standard and its utility as an international instrument would be negated if it did not satisfy the third country provisions in the EU Directive.[27]

The potential development by ISO of an international privacy standard was ultimately abandoned in 1998. AHAG concluded that at the time it would be premature for the ISO to consider developing an international data protection standard.[28]

[27] Chapter IV.

[28] See: Greenleaf, *Global Protection of Privacy in Cyberspace – Implications for the Asia-Pacific*, 16 June 1998, <http://austlii.edu.au/itlaw/articles/TaiwanSTLC.html>.

4. Potential Features of an International Convention

4.1. Content Issues

While the concept of personal data protection is frequently referred to as privacy in Australia, it is clear that an international convention will not use similar terminology. The definition of privacy varies by culture and the concept is quite expansive in its scope. Personal data protection on the other hand is a more tangible and static concept. Common themes have already emerged in national and regional laws, international guidelines and codes of conduct on how personal information should be processed. These include:

- Accountability;
- Access;
- Purpose of collection;
- Knowledge and consent;
- Limited collection;
- Use and disclosure;
- Retention;
- Completeness, accuracy and currency; and
- Data security.[29]

These common principles provide the common footing necessary for the formation of an international data protection convention. The Montreux Declaration recognises similar commonalities and calls for the creation of a convention to universally recognise an individual's data processing rights.

Issues that may be of some controversy will be transborder flows and whether or not and in what form the sufficiency of data protection measures in states will be recognised. The effectiveness of an international convention rests on the strength of these provisions.

Agreement between the EU and the United States through the Safe Harbour framework has perhaps already solved one of the greatest stumbling blocks to garnering the international consensus needed for a convention. The exacting standard the EU Data Protection Directive imposes for information processing in third countries sets an enviable precedent for an international data convention. Nevertheless such a standard is necessary to maintain the integrity of personal data, the rights of the data subject and to ensure consistency in the way data is processed. In any case it is highly unlikely that EU member states will agree to a convention that offers a lower standard of protection than the standard already offered in the Data Protection Directive.

[29] Bennett, *An International Standard of Privacy Protection: Objections to the Objections,* 23 February 2004, <http://web.uvic.ca/polisci/bennett/pdf/ilpf.pdf>.

4.2. Practical Impact

Perhaps one of the most significant impacts of an international data protection convention is the effect it will have on domestic law. The convention will have a significant impact on international transactions and transborder data flows. However, it is unlikely countries will want different regimes for internationally and locally processed data. Therefore in implementing a convention it is likely domestic laws will be amended to avoid a duality of regimes and the inefficiencies and inconvenience that would result from having two privacy laws.

The convention will in all probability emerge as a default standard for privacy protection. Some countries may be forced to implement measures compatible with the convention in order to engage in certain transactions.

Another significant impact of a convention is that it may resolve data processing differences between the EU and the United States. However, such a resolution may occur even without a convention, as the United States seems to be moving closer to laws consistent with those in the EU. There is already support from key industry groups for comprehensive national privacy legislation to replace the patchwork of state and federal laws currently operating in the United States.[30]

While a convention will resolve inconsistencies between the EU and the United States, its unifying impact will of course be much broader than this. It will create an international regime for data processing that can potentially ensure proper data protections are applied to the vast majority of cross border transfers. Ensuring not only the adequacy of trans-Atlantic data protections but also data flows between other continents. An international data protection convention will essentially create a global network that allows borderless transfers while still maintaining individuals' privacy rights. There are a number of benefits of this, notably an increase in consumer confidence and trust in cross-border data flows. This will, among other things, help to allay concerns about the outsourcing of data processing, eg to international call centres.

An international convention is only one albeit a significant step towards universal data protection. As the Safe Harbour implementation study[31] demonstrates measures that aid implementation such as guidance and compliance advice is needed to ensure that *in practice* data is processed fairly. Privacy Enhancing Technologies (PETs) and other technical measures are also needed to guarantee compliance at a technical level. Lastly, a convention must be backed by both international and domestic enforcement provisions and compliance reviews to ensure it is correctly implemented. The development of an ISO standard once a privacy convention has been finalised may provide the technical guidance needed to aid practical compliance with a convention.

[30] See for example, *Microsoft Advocates Comprehensive Federal Privacy Legislation*, Mircosoft PressPass, 3 November 2005, <http://www.microsoft.com/presspass/press/2005/nov05/11-03DataPrivacyPR.mspx>.

[31] Asinari and others above note 12.

5. Conclusion

With the rapid pace at which technologies are advancing effectively creating a borderless society in which information flows freely between countries, there is clearly a need for a global approach to data protection standards. It should be emphasised that whilst the broad concept of privacy is used in Australia to describe the protection of personal information, an international convention would inevitably be referred to as a data protection convention, the more commonly accepted term worldwide. Existing data protection initiatives and the principles that they contain will no doubt shape the nature of such a convention. A UN data protection convention would serve to strengthen the universal nature of data protection principles and provide a foundation for unifying disparate approaches to data protection.