A WAY AHEAD FOR GLOBAL PRIVACY STANDARDS?
Thoughts on a UN Convention on Data Protection, International Standards and International Agreements. Which is the Best Option?

By Lauren Saadat and Shannon Ballard[1]

As published in the October 2007 issue of *Privacy Laws and Business*

There is ongoing discussion and debate by policy makers in both the private and public sectors on the necessity for international privacy related standards. In the private sector, compliance is an increasingly complex and difficult proposition, as jurisdictions throughout the world pass privacy legislation on the collection and use of personally identifiable information.

In the public sector, data protection authorities are frustrated by their inability to enforce laws against bad actors in foreign jurisdictions. Justice and security officials have, at times, been hampered by legislation that restricts personal information sharing for terrorism prevention.

IN THE BEGINNING

International recognition of privacy rights has existed for some time. Article 12 of the United Nations (UN) Declaration of Human Rights of 1948 is the first statement of privacy as a basic right by an international organisation. Article 12 states: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks." While the Declaration did not have the force of law, the proclamation was ratified with 48 votes in favour and zero against (eight abstentions – all Soviet Bloc states, South Africa and Saudi Arabia), thus setting the moral imperative for recognition of this right by all nations. Other regional declarations subsequently evolved, including the Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms of 1950. Article 8 of the Convention outlined the right to respect for private and family life.

In 1980 the Organization for Economic Cooperation and Development (OECD) went further than the previous declarations. It issued the Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, which set out principles with explanations. More than half of its members at the time were introducing privacy protection laws, so one major goal was to prevent restriction of crossborder flows of personal information. In 1981, the Council of Europe negotiated the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, which obliged the signatories to enact legislation concerning the automatic processing of personal data. This was followed by the European Union Data Protection Directive, a detailed set of rules under which each Member State has issued national privacy legislation. Most recently, Asia Pacific Economic Cooperation (APEC), an organisation of 21 member economies, endorsed its Privacy Framework in 2004. The Privacy Framework is consistent with the core values set out in the OECD Guidelines but more detailed.

HOLDING HANDS AROUND THE WORLD? WELL, NOT QUITE

---

[1] Lauren Saadat and Shannon Ballard are Associate Directors of International Privacy Policy for the US Department of Homeland Security's Privacy Office.

Privacy protection and the importance of information flows has garnered global attention by policy makers for some time. However, these pronouncements and guidelines have had mixed success.

The OECD guidelines, the EU Directive, and the APEC Privacy Framework are all based on the Fair Information Principles (FIP), a set of principles first articulated as a result of a 1973 report by the US Department of Health, Education, and Welfare advisory committee that identified eight practices, known as the FIP. But subtle differences in how these principles are interpreted and applied, as well as different structures of government and legal systems, have resulted in varying and even conflicting implementation. Statements and guidelines appear insufficient to make national authorities comfortable with citizens' information flowing outside of their jurisdiction. Even within the EU, there is ongoing debate about the degree to which national authorities will rely on one another's conclusions over Binding Corporate Rules and sharing of law enforcement databases. However, despite the numerous statements recognizing privacy as a right and several detailed guidelines, there has been a renewed call for a global standard on data privacy issues.

The International Conference of Data Protection and Privacy Commissioners (ICDPPC), a group of independent national and sub-national authorities, issued the Montreux Declaration in 2005. It should be noted that the ICDPPC Euro-centric membership criteria defines what an independent data protection authority is. As a result, that group is not representative of a full cross-section of international privacy views. In fact, several nations that have privacy legislation are not ICDPPC members, including the US. The Montreux Declaration called for the UN to prepare a binding legal instrument to "formally declare data protection and privacy as enforceable human rights". This was reiterated during the 2006 ICDPPC meeting in London, with its resolution for commissioners to "support the need of an International Convention and the development of other global instruments" to address privacy problems. Interestingly, the resolution for the September 2007 ICDPPC meeting in Montreal did not call for a UN instrument, but rather called for the Commissioners to "support the development of effective and universally accepted international privacy standards" as created by the International Organization for Standardization (ISO). The ISO is a network of the national standards institutes of 157 countries, on the basis of one member per country. While the ISO defines itself as a non-governmental organisation (NGO), its ability to set standards that often become law, either through treaties or national standards, makes it more powerful than most NGOs.

THE GOLDEN RULE

Would an ISO standard on privacy result in increased trust and facilitated cross-border transfers of personally identifiable information? Based on past history, this is unlikely. Rather than a new privacy standard, the future of cross-border privacy will likely depend on bilateral or multilateral agreements based on reciprocity and accountability.

Reciprocity is defined as exchanges of roughly equivalent values in which the actions of each party are contingent on the prior actions of the others in such a way that good is returned for good, and bad for bad. Some commentators have declared that reciprocity is a "condition that theoretically attaches to every legal norm of international law". Indeed, it is a fundamental structure of many international agreements, including arms control, trade and commerce, and law

enforcement. When signing a bilateral or multilateral agreement, one holds the other accountable for the implementation of and enforcement of that agreement. Mutual recognition of the other's ability to oversee and be accountable to these actions is intrinsic to such an agreement.

There are some notable examples of how reciprocity has worked. Under the bilateral US-EU Passenger Name Records (PNR) Agreement, the US and EU have committed to reciprocal treatment of travelers' airline reservation information used for homeland security purposes. Multilateral agreements also show promise. The Regional Movement Alert List (RMAL), a regional initiative within APEC to share lost and stolen passport information, is based on reciprocity. APEC members are also working on cross-border privacy rules that will implement its Privacy Framework and create an accountable system for personally identifiable information moving across the Asia-Pacific region for commercial purposes.

OKAY, NOW WHAT?

Is it possible to achieve a global standard with buy-in from all nations? As this piece goes to publication, Google's Global Privacy Counsel briefed reporters on Google's proposal to "create minimum global standards, partly by law and partly by self-regulation". This proposal seems to apply strictly to the private sector. Based on the APEC Framework, it has already met resistance because of its focus on actual harms to consumer privacy, a point of divergence in several countries' legislation. For any standard to be broadly adopted by the public and private sectors, it will have to reflect the values of those nations that handle a substantial amount of personal information. This is a lofty goal.