INTERNATIONAL PRIVACY STANDARDS: A CONTINUING CONVERGENCE

COLIN J. BENNETT, DEPARTMENT OF POLITICAL SCIENCE, UNIVERSITY OF VICTORIA, BC, CANADA.

cjb@uvic.ca

Visiting Professor, School of Law, University of New South Wales

In 1992, I published a book entitled "Regulating Privacy: Data Protection in Europe and the United States" which argued that throughout the 1970s ad 1980s there had been a progressive convergence of information privacy policy throughout advanced industrial states.[1] Although there were significant differences in the ways that laws were implemented and enforced, the principles of information privacy, commonly known as fair information principles, were progressively influencing both domestic law and international agreement. The codification of these principles varied, and continues to vary, but the trend was toward higher levels of convergence.

I later argued that this trend continued throughout the 1980s and 1990s. As more and more countries passed these laws, they continued to draw lessons from the pioneers about what worked, and what did not. Supervisory authorities learned from one another. The repertoire of regulatory, self-regulatory and technological policy instruments was increasingly evident in an expanding number of countries. Particular instruments were no longer confined to the administrative regimes of individual states. They were part of the international toolkit, to be applied wherever and whenever.[2]

Over the last decade, however, we have seen an increasing set of concerns that the international privacy protection project has been unraveling. More and more commentators have pointed to the discrepancies between information privacy policies. More and more multi-national companies have emphasized the difficulty of having to comply with different rules in different jurisdictions, with the associated transaction costs that have to be passed along to consumers. In part, these complaints about the differences have motivated new international projects and standards in an effort to ease the regulatory burdens and promote better cross-national harmonization.

The 2009 paper from the Galway Project, for example, argues for a new accountability approach that "will help bridge approaches across disparate regulatory systems, by allowing countries to pursue common data protection objectives through very

---

[1] Colin J. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca: Cornell University Press, 1992.

[2] Colin J. Bennett and Charles D. Raab, *The Governance of Privacy: Policy Instruments in Global Perspective,* Cambridge: MIT Press, 2006.

different — but equally reliable — means."[3] When the APEC Privacy Framework was first endorsed by APEC ministers in November 2004, it was heralded as an attempt to promote a "consistent approach to information privacy protection across APEC member economies, while also avoiding the creation of unnecessary barriers to information flows." The US Secretary of State "warned APEC ministers that a multiplicity of privacy standards could create confusion in the marketplace and impede the information flows that are vital to conducting business in a global economy."[4]

Most recently, the international data protection commissioners have agreed to a set of "International Standards for the Protection of Personal Data and Privacy," the explicit purpose of which was to "define a set of principles and rights guaranteeing the effective and *internationally uniform protection of privacy* with regard to the processing of personal data (my emphasis)"[5] It remains to be seen how this agreed standard will develop in the years ahead, and in particular whether it will form the basis for a full-fledged international convention negotiated through the United Nations, as some hope. Nevertheless, it is instructive that the Commissioners felt the need to negotiate a further instrument, beyond the EU Directive, the OECD Guidelines and the Council of Europe Convention, to promote further harmonization of law and policy. At the same conference, speaker after speaker emphasized the extraordinary difficulty of determining applicable law and standards under conditions of globalization, and especially within a "cloud-computing" environment.

I do not want to minimize the intricate compliance issues that corporations and their lawyers need to navigate through international data protection law. Nor do I want to suggest that there are not some considerable differences in enacted and proposed data protection laws, and in their implementation. Definitions, approaches, requirements and obligations vary; it can be no different. On the other hand, I do contend that the assumption that international data protection is "unraveling" as more and more countries enact laws is wide of the mark.

This policy issue has come a remarkable long way since 1970, when the state of Hessen enacted the first modern data protection state, and appointed the first data protection commissioner, Spiros Simitis. Over sixty national or sub-national jurisdictions now have data protection statutes. Looking historically and admittedly from the vantage point of the high-flying aircraft, there has been a remarkable diffusion of these laws, and

---

[3] Centre for Information Policy Leadership, "Data Protection Accountability: The Essential Elements," October 2009 at: http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf

[4] "APEC Ministers endorse the APEC Privacy Framework," November 20, 2004 at: http://www.apec.org/apec/news__media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html

[5] The Madrid Resolution, *International Standards on the Protection of Personal data and Privacy*, November 5th, 2009: http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

convergence around some very simple and common principles. There is now a broad consensus about what it means for the responsible organization to protect personal data and to respect the privacy of the individual. Forty years ago, there was not that consensus.

There has also been a diffusion of supervisory authorities. The *Privacy Laws and Business* website currently lists 45 countries as having established national supervisory data protection agencies; there are also of course a number of sub-national authorities in federal jurisdictions.[6] Not all of these authorities perform data protection responsibilities exclusively. Some may not have the desired degree of independence. But this does constitute a large, and expanding, policy community. No authority that I know of has ever been removed. The independent supervision of these laws, admittedly with a varying blend of functions, is institutionalized – nationally and cross-nationally.

These trends are also, of course, influencing the policy-making process in countries that have yet to pass legislation. At a conference in Sydney on March 3-4, 2010, representatives from several Asia-pacific countries convened to discuss their respective laws, both enacted and intended. I was struck at the extent to which these regional laws were been influenced by developments in other parts of the world. Academics from Malaysia, the Philippines, Thailand and South Korea each reported that their proposed legislation was influenced by a variety of national and international instruments; the 1995 European Union Directive, the 1980 OECD Guidelines, the 1981 Council of Europe Convention, as well as national legislation in Europe, Canada, Australia and elsewhere. The 2005 APEC Privacy Guidelines were explicitly developed as a model for countries in this region. They have clearly had an influence, but they are one influence among many. This diversity of influences also is apparent in the new Mexican data protection law, which applies information privacy principles to both public and private sectors for the first time.

It is simply not true that there are different regional "models" for information privacy law. Each state draws upon influences from many places, and from a global repertoire of solutions. A variety of factors, national and international, motivate the passage of legislation and shape the content of law. Some ideas have gone out of fashion. For instance, few new laws contain provisions for the negotiation of codes of practice. Few require registration of databases with the supervisory authority. And each includes the basic information privacy principles. There are variations, to be sure. But the essential elements are all there.

Furthermore, this convergence is not only motivated by the desire to be labeled "adequate" by the European Commission. The principles also flow from the logic of the problem or from the "deep grammar of the subject" as the late UK privacy expert, Paul Sieghart once said.[7] If one accepts the overriding policy goal that individuals should be provided in law a greater level of control over the information that relates to them, then the policy outcomes cannot logically be too different. However worded, they must be told why their information is being collected. They must be given legal assurances that

---

[6] http://www.privacylaws.com/templates/Links.aspx?id=404

[7] Quoted in Bennett, *Regulating Privacy.*

only relevant or proportionate information is being processed. They must be given assurances that it will not be used or disclosed in ways inconsistent with those purposes. They must be given rights to access that information, and to correct it if it is inaccurate. They must be assured that the information will be held securely. They must have rights to object and complain. All information privacy law contains obligations for organizations and rights for data subjects. Variations tend to be centered on matters of implementation and definition, crucial to be sure, but not fundamental to the overriding policy goals.

So I am not persuaded that a thorough review of the 1980 OECD Guidelines is necessary, as is being contemplated. I fear that such a review would take a long time, and would end up with a set of principles which are not substantially different from the current version. I am also not persuaded by those who, because of new technology or eroding national jurisdictions, would seek new solutions embraced by the term "accountability" which "shifts the primary responsibility for data protection from the individual to the organization collecting and using data." [8] Accountability is within the very fibre of information privacy policy. The central issue is what it means in practice.[9]

In conclusion, therefore, I still see a trend towards policy convergence. To coin a horribly trite metaphor: information privacy is not rocket science, at least for the vast majority of data users. More and more organizations in more and more countries have to: be open about their policies and practices; only collect personal information for defined and relevant purposes; only use and disclose that information in ways that are consistent with those purposes; grant access and correction rights to individuals; and keep the data secure. And those principles should apply regardless of the institution, and regardless of the technology.

When viewed historically, the progressive convergence of information privacy policy is still continuing. Discrepancies in law are real, but they should not be exaggerated. They certainly should not be cited as evidence that completely new approaches to the problem are needed. If one looks for discrepancies, one will find them. But we should also recognize the considerable commonalities.

---

[8] Ibid., p. 10..

[9] The next issue will include an analysis of the accountability approach