INTERNATIONAL PRIVACY STANDARDS: CAN ACCOUNTABILITY BE ADEQUATE?

Colin Bennett

Department of Political Science

University of Victoria

Victoria, BC. Canada

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

Draft for Privacy Laws and Business International.

In the last issue, I wrote about the continuing convergence of international data protection policy. Here I want to focus on implementation. Over the last year or so, the debate on international data protection has become somewhat polarized between those who would continue to support the EU approach, essentially a prohibition on transfers to countries which do not have an "adequate level" of data protection, and the "accountability approach" which focuses more on the protection afforded by individual data controllers. There is a common perception that the "adequacy regime" has been ineffective, despite the fact that it continues to motivate "third countries" to line up for the Commission's adequacy stamp of approval. The process appears too slow, too secretive, too legalistic, and based on the flawed assumption that "adequate law" means "adequate protection." There are "adequate" organizations in "inadequate" jurisdictions, and just as there are "inadequate" organizations in "adequate" jurisdictions. So how does one determine the "adequacy" of an organization's practices?

I was part of a team that wrote a contract report for the EU Commission in 1999. We were asked to look at precise and "real world" data transfers in a number of sectors to six "receiving jurisdictions" (US, Japan, Hong Kong, Australia, New Zealand and Canada). We wrote a series of case studies, and assessed the protections in force in these countries at the time. Our most prominent recommendation: "We believe that a more empirical analysis of policies and practices, and not just of legal norms and rules, serves both to advance the debate and to anticipate the specific problems that will be encountered in the implementation of the Directive. The assessment of adequacy will be incomplete to the extent that it cannot assess actual practices and the realities of compliance."[1] The purpose of this brief commentary is to try advance the debate about how we can assess

actual practices, and render organizations truly "accountable" especially when their operations are offshore. I want to suggest that approaches to accountability should not be regarded as alternatives to the adequacy approach, but as complements to it.

The Many Meanings of Accountability

Scholars of public administration have spilled a lot of ink considering the many meanings of the word "accountability." However, there seems to be a consensus that the process must involve being called "to account" by some authority for one's actions. The involvement of an external body is, therefore, indispensable. Accountability implies a process of transparent interaction, in which that body seeks answers and possible rectification. That external agent is presumed to have rights of authority over those who are accountable – including the rights to demand answers and impose sanctions. Thus, if there is no possibility of external compulsion to change practices, there can be no accountability.

Furthermore, accountability means more than "responsibility." One can always act "responsibly" without reference to anyone else. Accountability is always directed towards an external agent; responsibility is not. Accountability is also more than "responsiveness." For example, the responsiveness of a company to its customers is a desirable component of accountability, but again does not imply that there is external accountability. Accountability is not present simply because consumers have an option of choosing another company in a competitive marketplace.

The literature is, of course, far more complex, but these seem to be the central elements.[2] There must be a common understanding *of who is accountable, for what and to whom.*

Accountability and Privacy

The vagueness of the term is reflected in its usage in the field of privacy law. There is, of course, an accountability principle within the OECD Guidelines: "A data controller should be accountable for complying with measures which give effect to the principles stated above." The Guidelines go on to explain that "it is essential that under domestic law accountability for complying with privacy protection rules and decisions should be placed on the data controller who should not be relieved of this obligation merely because the processing of data is carried out on his behalf by another party, such as a service bureau."[3] But nowhere is the "to whom" question specified.

The theory of accountability within the APEC framework is subtly different: "A personal information controller should be accountable for complying with measures that give effect to the Principles stated above. When personal information is to be transferred to another person or organization, whether domestically or internationally, the personal information controller should obtain the consent of the individual *or* exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles." Note that these are alternatives. And who determines the "due diligence" or the "reasonableness" of the steps? Again the "to whom" dimension is not specified, although the precise role for various "accountability agents" is now being addressed through the Pathfinder project for a Cross Border Privacy Rules System within APEC.[4]

The 2009 Madrid international privacy standard includes an Accountability Principle:

> The Responsible person shall: a) Take all the necessary measures to observe the principles and obligations set out in this Document and in the applicable national legislation, and b) Have the necessary internal mechanisms in place for demonstrating such observance both to data subjects and to the supervisory authorities in the exercise of their powers, as established in section 23 (Monitoring).

Here the "to whom" element is specified. Organizations are accountable to both data subjects and supervisory authorities. And the Article 29 Working Party has also supported the inclusion of an accountability principle in any revision of the Directive: "it would be appropriate to introduce in the comprehensive framework an accountability principle, so data controllers are required to carry out the necessary measures to ensure the substantive principles and obligations of the current Directive are observed when processing personal data, and to have the necessary internal mechanisms in place to demonstrate compliance to external stakeholders, including DPAs.[5] And who are these other "external stakeholders"?

The discussion paper (dated October 2009) from the Centre for Information Policy Leadership – the "Galway Project" -- is premised on the need to shift "the focus of privacy governance to an organization's ability to demonstrate its capacity to achieve specified objectives" and "vesting the organization with both the ability and the responsibility to determine appropriate, effective measures to meet those goals."[6] The approach requires "that organizations that collect, process or otherwise use personal data take responsibility for its protection and appropriate use *beyond mere legal requirements*,

and are accountable for any misuse of the information that is in their care" (my emphasis). A plea for "adaptability" also appears: "An accountability approach enables organizations to adopt methods and practices to reach those goals in a manner that best serves their business models, technologies and the requirements of their customers." The Galway paper addresses many of the relevant questions, but still leaves several unanswered, although I understand that the project is still underway,

Accountability for What and to Whom?

So what criteria do accountability arrangements have to satisfy in order for them to provide adequate privacy protection? One thing is clear. Accountability should never be a replacement for liability. If individuals are harmed as a result of the inappropriate collection, processing or disclosure of their personal information, than any amount of "due diligence" should never substitute for that individual's ability to seek and obtain redress. Failure of accountability must readily result in liability.

But accountable for what? In a 1995 report to the Canadian Standards Association,[7] I made a rough distinction between the accountability of *policy*, of *procedures*, and *practice*. Many current accountability mechanisms simply focus on the first, the stated privacy policies, and compare what is said on a website, or in a code of practice, to a stated norm. Claims of compliance are based on an analysis of words, rather than processes or practices. Most privacy seal programs operate at this level.[8] This might be appropriate for some organizations, but not for others. A deeper set of questions relates to internal mechanisms and procedures: does the organization have an effective

complaint handling process? Is there a responsible person, such as a Chief Privacy Officer? Is there a privacy management framework? Is there staff training?

Few organizations, however, subject themselves to a verification of practices. Do the policies work? Is privacy protected? At this level, it is difficult to see how accountability of practice can be satisfactorily claimed without external and independent auditing. Privacy auditing has been around for a long time, but there is little evidence that market pressures alone will push this kind of external conformity assessment around the international economy. There are other motivations, however. Data protection authorities might begin to insist on external audits as necessary components of compliance investigation and reporting. An overlooked element of the recent decision by the Canadian commissioner against Facebook was the company's agreement to have its processes subjected to a full technical audit within a year.[9] Privacy auditing can be quite easily attached to broader financial or management audits, when for instance the firm is being considered for registration to a quality assurance standard, such as ISO 9001.[10]

Data protection authorities cannot be the only agents of accountability, because they do not have sufficient resources and do not exist in every country. They must rely on surrogates, including a complicated array of private sector actors with different levels of competence and independence: accounting firms, standards bodies, seal and trustmark programs, mediation and dispute resolution bodies and so on. There is a key role for the data protection authorities to send a clear message to data users (public and private) on the acceptability of different third-party accountability mechanisms, and about what doing "due diligence" should mean in different contexts. That message should also signal

that such actions would be given evidentiary value in any investigative or enforcement procedures concerning that data user. There has been a start in that direction, with the publication of model contracts, and the approval of certain binding corporate rules, although neither necessarily obliges an independent testing of practices. A further step is the explicit use by DPAS of the suite of security standards and instruments in the ISO 27001 series, to which any organization anywhere might be certified, and thus be audited.[11]

"Accountability" is not, then, a separate approach to data protection. It has always been within the very fibre of these laws. Neither is it an alternative to adequacy assessments in the cross-border context. Rather accountability instruments are ways to make the adequacy framework work more effectively. We have moved beyond, however, a situation where the only acceptable "account" of what happens to personal data within organizations is that provided by the organization itself. The "trust me, my account is the truth" approach will not be sufficient for many organizations. The task is to build verifiable accountability instruments into the implementation of privacy law. And those mechanisms will be necessary regardless of whether personal data is held within a defined jurisdiction, or crosses geographic borders.

[1] Application of a Methodology designed to Assess the Adequacy of the Level of Protection of Individuals with regard to Processing Personal Data: Test of the Method on Several Categories of Transfer (European Commission Tender No. XV/97/18/D, September 1998) (With Charles D. Raab, Robert M. Gellman and Nigel Waters) at:
http://ec.europa.eu/justice_home/fsj/privacy/docs/studies/adequat_en.pdf
[2] See, Richard Mulgan, "Accountability: An Ever-Expanding Concept? *Public Administration*. Vol. 78. No 3, 2000 (pp. 555-573).
[3] OECD, *Guidelines for the Protection of Personal Information and Transborder Data Flows,* (Paris: OECD, 1981) at:
http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html
[4] APEC Privacy Framework at:
http://www.apec.org/apec/news__media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html
[5] Article 29 Data Protection Working Party, *The Future of Privacy,* Adopted December 01, 2009 at:
http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2009_en.htm
[6] Center for Information Policy Leadership, "Data Protection Accountability: The Essential Elements" October 2009 at:
http://www.huntonfiles.com/files/webupload/CIPL_Galway_Accountability_Paper.pdf
[7] See for example, Colin J. Bennett, "Implementing Privacy Codes of Practice" (PLUS 8830), Canadian Standards Association, 1995.
[8] Galexia, *Trustmark Schemes Struggle to Protect Privacy* (2008) at:
http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.html
[9] Privacy Commissioner of Canada, PIPIEDA Case Summary, CIPPIC v. Facebook at:
http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm
[10] Colin J. Bennett and Robin M. Bayley, *Saying what you do, and Doing what you say: Arguments and Prospects for an International Privacy Standard.* Paper Prepared for the annual meeting of the International Data Protection Commissioners, Terra Incognita, Montreal September 25th-28th, 2007 at: http://www.privacyconference2007.gc.ca/workbooks/pres_wrkshop2_01_bennett_e.pdf
[11] http://www.iso27001security.com/