International privacy standards: a continuing convergence

Colin J. Bennett

June 2010

International privacy standards: a continuing convergence

A thorough review of the 1980 OECD Guidelines is not necessary, argues **Colin Bennett**. While there are differences, considerable commonalities between national laws exist.

In 1992, I published a book entitled *Regulating Privacy: Data Protection in Europe and the United States*, which argued that throughout the 1970s and 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 emphasised 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 harmonisation.

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 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 harmonisation of law and policy. At the same conference, speaker after speaker emphasised the extraordinary difficulty of determining applicable law and standards under conditions of globalisation, and especially within a "cloud-computing" environment.

I do not want to minimise 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 remarkably long way since 1970, when the state of Hessen enacted the first modern data protection statute, 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 convergence around some very simple and common principles. There is now a broad consensus about what it means for the responsible organisation 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 & 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 independ-

ence. 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 institutionalised – 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 3-4 March 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 being 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 (p.1), 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 labelled "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 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 organisations 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 organisation 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 organisations 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 recognise the considerable commonalities.

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.

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," 20 November, 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, 5 November 2009: http://www.privacyconference2009.org/dpas_space/space_reserved/documentos_adoptados/common/2009_Madrid/estandares_resolucion_madrid_en.pdf

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

7 Quoted in Bennett, *Regulating Privacy*.

8 Ibid., p. 10.

9 The next issue of *PL&B International* will include an analysis of the accountability approach.

AUTHOR

Colin J. Bennett is Professor at Department of Political Science, University of Victoria, BC, Canada, and Visiting Professor, School of Law, University of New South Wales, Australia. Email: cjb@uvic.ca

INTERNATIONAL NEWSLETTER

PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

German employers may gain employee monitoring powers

New employment rules, to be debated in the legislature next month, may change the playing field dramatically, says **Laura Linkomies**.

On 1 June, a new draft was published for the chapter on employee data protection. This chapter will, if adopted, be inserted into the Federal Data Protection Law and thus form the basis for processing employee data.

"The current provisions in s.32 of the Federal DP Act are an interim solution," said Dr Sabine Grapentin, partner at law firm Noerr. "These provisions that apply since 1 September 2009 are important as previously there were no specific provisions on employee data. However, while they reiterate old data protection principles, the new draft law contains many more details."

Speaking at a *Privacy Laws & Business* Briefing in Frankfurt at the beginning of June, Grapentin said that rules on collection and use of employee data for the detection of criminal offences are strict. "As long as s.32 appplies, there is considerable uncertainty regarding the lawfulness of compliance measures which aim at exposing criminal offences. The new chapter to the federal law seeks to

Continued on p.3

Mexico passes Federal DP law

Companies trading in Mexico need to prepare to stay within the law. **Lina Ornelas** and **Katitza Rodriguez** analyse the new rules.

Data protection law in Mexico has undergone several developments in recent years. In 2009, the Mexican Constitution was amended to recognise data protection as a fundamental and autonomous right (articles 16 and 73). In April 2010, the Mexican Senate passed the Federal Data Protection Act.

The Mexican Constitution establishes that every person can exercise his or her ARCO rights (access, rectification, cancellation and opposition) under the exceptions set out by law, for reasons of national security, public order, security, public health (Article 16). The Constitution also empowers the Mexican Congress to pass legislation to protect personal data in the possession of private entities (Article 73).

Continued on p.4

Issue 105 **June 2010**

NEWS

2 – Comment
Employment and globalisation

News
Data exports from Germany under Safe Harbor face obstacles • IP addresses not personal data says Irish court • UK government's privacy overhaul • UK approves JP Morgan Chase and BP BCR • France: CNIL orders military supply company to stop using biometric employee ID • Google, Microsoft and Yahoo do not comply, Article 29 Group says • Spain's Data Protection Agency imposes €24.8 million in fines • US FTC drafts business privacy principles • CNIL stops employee video surveillance

NEWS

7 - US and French courts rule on private use of company IT
17 - Korean court upholds union membership sensitivity
18 - Privacy Commissioners form global network and warn Google
19 - Google StreetView challenged

LEGISLATION

5 - Germany: fighting unfair competition citing DP breaches
9 - Poland: Consent and employees' biometric data
10 - Ireland close to mandatory data breach notification

MANAGEMENT

11 - Data leakages from old IT equipment threaten compliance
20 - Privacy in the Cloud: 16 points to consider about cloud computing

ANALYSIS

13 - International privacy standards
15 - Data surveillance in India

INTERNATIONAL newsletter
ISSUE NO 105 JUNE 2010

PUBLISHER
Stewart H Dresner
stewart@privacylaws.com

EDITOR
Laura Linkomies
laura@privacylaws.com

LEGAL EDITOR
James Michael
james.michael@privacylaws.com

ASIA-PACIFIC EDITOR
Professor Graham Greenleaf
graham@austlii.edu.au

NEWSLETTER SUBSCRIPTIONS
Glenn Daif-Burns
glenn@privacylaws.com

CONTRIBUTORS
Lina Ornelas
Federal Institute for Access to Public Information, Mexico
Katitza Rodriguez
Electronic Foundation Frontier
Dr Vera Jungkind
Bristows
Xawery Konarski
Traple Konarski Podrecki & Partners, Poland
Dr Grzegorz Sibiga
Traple Konarski Podrecki & Partners, Poland
Dugie Standeford
PL&B Correspondent
Professor Whon-il Park
Kyung Hee University, South Korea
Professor Colin J. Bennett
University of Victoria, Canada
Annelies Moens
Australasian Legal Information Institute

PUBLISHED BY
Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, United Kingdom
Tel: +44 (0)20 8868 9200
Fax: +44 (0)20 8868 5215
Website: www.privacylaws.com

The *Privacy Laws & Business* International Newsletter is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of the newsletter. Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given. No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior permission of the publishers.

Design by ProCreative +44 (0)845 3003753
Printed by Printflow Ltd +44 (0)20 7689 8697

ISSN 0953-6795

comment

Employment personal data rights and globalisation

It has now been just over 10 years since Scott McNealy of Sun Microsystems famously (or notoriously) said: "You already have zero privacy – get over it." It was an overstatement, at least in terms of data protection and labour laws in some countries. As explained at *PL&B*'s Privacy Officers Network meeting in Frankfurt on 1-2 June, Germany is now in the process of modifying its data protection and labour laws to allow employers to process somewhat more (but not just any) information on employees (p.1).

Meanwhile, the Polish Supreme Court has ruled that employers can only demand a limited range of personal information from employees and job applicants, and emphatically cannot require biometric data (p.9). A French court allows employers to access employees' emails, so long as they are not marked "*privé*", while the New Jersey Supreme Court has ruled that an employer cannot ever look at emails from an employee to a lawyer on company IT equipment, even if there is an absolute ban on personal use. The US Supreme Court is about to rule on the privacy (or not) of government employees' pager use. (p.7)

There are always new international developments in data protection law, either by legislation, as in the form of Mexico's new data protection law (p.1), India's various new laws on data surveillance (p.15), Ireland's proposals for data breach notification (p.10) or litigation, as in the interesting application of competition law to data protection in the German courts (p.5). As data protection standards creep (and sometimes lurch) towards global harmonisation, Colin Bennett argues that there is already substantial convergence, and that a review of the 1980 OECD guidelines is not necessary (p.13). The development of cloud computing (p.20) has made the development of global standards even more pressing.

Globalisation also has received a boost in the alliance of 10 national data protection authorities from around the world to form a Global Privacy Enforcement Network (GPEN), starting with a joint rebuke to Google for merging Google Buzz with private Gmail addresses (p.18). Google has also come in for criticism from several national authorities for collecting open wi-fi information in Street View. For a response from Google in the person of its Global Privacy Counsel, to hear from four of the 10 GPEN DP authorities, how to get approval for a biometric identification technique, and three days of equally relevant presentations and discussion, come to *PL&B's* 23rd Annual International Conference in Cambridge on 5-7 July.

James Michael, Legal Editor
PRIVACY LAWS & BUSINESS

Contribute to PL&B newsletters

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Your Newsletter Subscription **Includes**

1. Six Newsletters a year
The *Privacy Laws & Business (PL&B) International Newsletter*, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from 50 countries – new laws, bills, amendments, codes and how they work in practice.

2. Helpline Enquiry Service
Subscribers may telephone, fax or email us with their questions such as: contact details of Data Protection Authorities, the current status of legislation and amendments, and sources for specific issues and texts.

3. Email updates
We will keep you informed of the latest developments.

4. Index
Subscribers receive annually a cumulative Country, Subject and Company index. Multiple headings include advertising, data security, Internet, police, transborder data flows and sensitive data. The index is updated after every issue on our website www.privacylaws.com.

e-Newsletter

Electronic Option
The newsletter is available in PDF format either for use in one office or for uploading onto your Intranet or network. This format enables you to see the Newsletter on any computer on your network as it appears in the paper version. It allows you to print out pages at any location.

Privacy Laws & Business has clients in over 45 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the Financial Times *lists; and 10 of the Global Top 20 in the Fortune list.*

Privacy Laws & Business also publishes the United Kingdom Newsletter, a publication, which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.

Newsletter Subscription Form

Subscription Packages

(Please add 17.5% VAT to prices for the PDF format within the EU).

❑ **Print** ❑ **PDF** (please tick preferred delivery format)
❑ Send a FREE sample of the *UK/International* newsletter
❑ *PL&B International* Subscription **£375**
❑ *UK/International* Combined Subscription **£595** or an extra **£310** for existing UK subscribers)
❑ Special academic rate – 50% discount on above prices

Multiple Subscription Discounts
❑ 2-9 copies: 30% discount (indicate no. of copies ...)

Intranet Enterprise Licence for uploading onto your network (including additional printed copies)
❑ *PL&B International* **£1,875**
❑ *PL&B UK* **£1,425**
❑ Both *International/UK* newsletters **£2,975**
❑ I wish to receive *PL&B's* FREE email news service

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you *do not* wish to contacted by: ❑ Post ❑ Email ❑ Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

Payment Options

Address of Accounts (if different):

Postcode:

❑ Purchase Order
❑ Cheque payable to: *Privacy Laws & Business*
❑ Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

❑ American Express ❑ MasterCard ❑ Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature: Date:

I am interested in:
❑ Consultancy/Audits
❑ In-House Presentations/Training
❑ Recruitment Service

Please return to: Newsletter Subscriptions Department, Privacy Laws & Business, 2nd Floor, Monument House, 215 Marsh Road, Pinner, Middlesex HA5 5NE, UK, Tel +44 20 8868 9200
Fax: +44 20 8868 5215, email: info@privacylaws.com 16/6

www.privacylaws.com

Guarantee

If you are dissatisfied with the newsletter in any way, the unexpired portion of your subscription will be repaid.