galexia

– Benchmarks for Global Privacy Standards (November 2009) –

(Working paper – comments welcome)

Chris Connolly[1]

[1] Chris Connolly is an independent privacy consultant and researcher based at Galexia in Sydney, Australia. <http://www.galexia.com.au>.

© Galexia Pty Ltd.
Email: consult@galexia.com **Web:** www.galexia.com **Ph:** +612 9660 1111 **Fax:** +612 9660 7611
Post: Suite 98 Jones Bay Wharf, 26-32 Pirrama Road, Pyrmont NSW 2009, Australia

Contents

Document Control

Document Purpose

This document is a working draft of proposed benchmarks for global privacy standards.

Comments are welcome, and can be directed to:

Chris Connolly (Director)
Galexia
Suite 98 Jones Bay Wharf
26-32 Pirrama Road, Pyrmont NSW 2009
Phone: +612 9660 1111
Fax: +612 9660 7611
Email: consult@galexia.com

1. Introduction

There is a proliferation of initiatives to develop or implement global privacy standards. This should come as no surprise, as privacy is an area where globalisation is a key issue. However, there may be dangers (particularly for consumers) in developing multiple, competing standards, without first establishing a clear set of benchmarks.

This article attempts to describe and compare some of the current global privacy initiatives. The article proposes a set of benchmarks for a global privacy standard, written from a consumer perspective.

2. Current global privacy initiatives

Privacy is a vital human right, recognised in all major international human rights instruments, including:

— Article 12, *The Universal Declaration of Human Rights*, 1948, <http://www.un.org/en/documents/udhr/>.

— Article 17, *The International Covenant on Civil and Political Rights*, 1966, <http://www2.ohchr.org/english/law/ccpr.htm>.

Information privacy rights are elaborated in more detail in other significant legal instruments, including:

— *OECD Guidelines on the Protection and Privacy and Transborder Flows of Personal Data*, 1980, <http://www.oecd.org/document/0,2340,en_2649_34255_1815186_1_1_1_1,00.html>.

— *Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, 1981, <http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm> and the *Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows*, 2001, <http://conventions.coe.int/treaty/en/treaties/html/181.htm>.

— *EU Directive 95/46/EC on the protection of individuals with regard to the processing of personal data* 1995, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

— *APEC Privacy Framework*, 2005, <http://www.apec.org/>.

Information privacy rights are also the subject of several new global initiatives, including:

— **International Data Protection Commissioners**
The *Joint Proposal for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data* (referred to in this article as the Data Protection Commissioners Standard) has been prepared by a Working Group of international Data Protection Commissioners, co-ordinated by the Spanish Data Protection Agency. It will be published in November 2009.

— **The Galway Project**
The Centre for Information Policy Leadership, through a process facilitated by the Office of the Irish Data Protection Commissioner, is working with a panel of experts to 'define the essential elements of accountability… and suggest additional work necessary to establish accountability as a trusted mechanism for information governance'. A draft working paper is available.

— **International Standards Organisation (ISO)**
The International Standards Organisation is considering several privacy related proposals. A Privacy Task Force made a series of Recommendations in September 2009, including a recognition that 'an ISO privacy standard is increasingly needed in the ever developing networked and distributed computing and communications environment'.

3. The consumer perspective

To ensure that a Global Privacy Standard actually delivers real benefits to the community, there is a need for a set of *Benchmarks* that represent the consumer perspective.

The right to privacy has been included in important declarations and initiatives by civil society representatives. Recent examples include:

— *The Asia-Pacific Privacy Charter*, working draft 1.0, 2003, <http://www.worldlii.org/int/other/PrivLRes/2003/1.html> [APPC].

— *'The Seoul Declaration' Civil Society – TUAC Declaration to the OECD Ministerial Conference on the Future of the Internet Economy*, Seoul, Korea, 16 June 2008, <http://thepublicvoice.org/events/seoul08/seoul-declaration.pdf>.

— *Global Privacy Standards for a Global World – The Civil Society Declaration*, Madrid, Spain, 3 November 2009, <http://thepublicvoice.org/madrid-declaration/>.

The new *Global Privacy Standards for a Global World – The Civil Society Declaration* is supported by numerous civil society organisations and privacy experts. It contains the following key principles:

> (1) Reaffirm support for a global framework of Fair Information Practices that places obligations on those who collect and process personal information and gives rights to those whose personal information is collected;
>
> (2) Reaffirm support for independent data protection authorities that make determinations, in the context of a legal framework, transparently and without commercial advantage or political influence;
>
> (3) Reaffirm support for genuine Privacy Enhancing Techniques that minimize or eliminate the collection of personally identifiable information and for meaningful Privacy Impact Assessments that require compliance with privacy standards;
>
> (4) Urge countries that have not ratified Council of Europe Convention 108 together with the Protocol of 2001 to do so as expeditiously as possible;
>
> (5) Urge countries that have not yet established a comprehensive framework for privacy protection and an independent data protection authority to do so as expeditiously as possible;

(6) Urge those countries that have established legal frameworks for privacy protection to ensure effective implementation and enforcement, and to cooperate at the international and regional level;

(7) Urge countries to ensure that individuals are promptly notified when their personal information is improperly disclosed or used in a manner inconsistent with its collection;

(8) Recommend comprehensive research into the adequacy of techniques that 'de-identify' data to determine whether in practice such methods safeguard privacy and anonymity;

(9) Call for a moratorium on the development or implementation of new systems of mass surveillance, including facial recognition, whole body imaging, biometric identifiers, and embedded RFID tags, subject to a full and transparent evaluation by independent authorities and democratic debate; and

(10) Call for the establishment of a new international framework for privacy protection, with the full participation of civil society, that is based on the rule of law, respect for fundamental human rights, and support for democratic institutions.

The *Civil Society Declaration* calls on countries to sign one specific global privacy standard – the *Council of Europe Convention 108* (together with the *Additional Protocol)*. However, the Declaration leaves the door open for the development of other global frameworks and initiatives.

The following section sets out the author's proposal for a set of benchmarks for global privacy standards, building on the principles in the *Civil Society Declaration*.[2]

4. Proposed Benchmarks

Global Privacy Standards should be assessed against the following *Benchmarks*. Use of the benchmarks will help to improve these initiatives and hopefully also to rationalise the large number of initiatives into fewer initiatives that have the potential to develop into an effective Global Privacy Standard.

The development of inadequate standards may be more dangerous than doing nothing, as they have the potential to mislead consumers about the level of privacy protection available, and they can be used to undermine current and future domestic initiatives – such as proposed privacy legislation in Asia, Africa, South America and the Pacific.[3]

[2] The proposed benchmarks are the personal proposal of the author, and do not represent the formal views of any other *Civil Society Declaration* signatories.

[3] Electronic Privacy Information Center and Privacy International , Privacy and Human Rights 2006, September 2006, <http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559458> [New edition available soon].

4.1. Benchmark 1 – Comprehensive Coverage

Protection of privacy rights should be comprehensive, with as few gaps and exceptions as possible.

A Global Privacy Standard should promote privacy protection that meets the following criteria:

1. Privacy protection should cover all organisations, rather than just those who register or sign up to self regulatory initiatives (codes, trustmarks etc.). Consumers find it difficult to tell who is 'in' or 'out' of most self regulatory regimes, and organisations change their status at will and without notice. Many organisations simply forget to renew registrations, and none of the current self regulatory initiatives maintain accurate and up to date lists of members.[4] Also, registration in voluntary schemes is extremely low, and falls even lower during difficult economic periods.

2. Privacy protection should cover all sectors, rather than distinguishing between the Government and the public sector, or being limited to particular industry sectors. There are significant difficulties for consumers in identifying current coverage in privacy law.[5]

3. Privacy protection should apply to all consumers – there should be no distinction between data regarding local citizens and data regarding overseas citizens.[6] Equally, there should be no distinction between individuals acting as consumers / citizens or individuals acting as employees.[7]

4. Privacy protection should minimise exemptions. It is recognised that some exemptions may be necessary for law enforcement, emergencies, and freedom of expression. However, there are several ways in which these exemptions can be minimised. For example, exemptions should be limited to the specific Privacy Principles which conflict with other public interests in specific contexts, rather than providing a blanket exemption for particular types of organisations or activities. Also, exemptions can, where they are justified, be subject to additional oversight requirements, such as a requirement for warrants. Some exemptions should be subject to a case-by-case public interest test, such as exemptions for journalists and media organisations.

5. Privacy protection should cover all data formats and all forms of communication. It is important to avoid arbitrary distinctions between online and offline data,[8] or restricting privacy protection to information that has been processed in a particular way.

---

[4] See Connolly C, *Privacy Trustmarks – don't be fooled*, (2009) Privacy Laws and Business International 98, pages 9-12.

[5] For example, in Australia only businesses with revenue of over $3 million are covered. How can a consumer identify this gap in protection? In Japan, only data sets with greater than 5,000 entries are covered. How can a consumer know how big the data set is?

[6] For example, some privacy and security laws in regions in China only cover data held on overseas citizens, held by local outsourcing companies. Conversely, some privacy laws do not adequately protect information on foreign citizens being processed or hosted in the jurisdiction.

[7] For example, employees are excluded from some parts of the Australian privacy law, and can also be excluded on a case-by-case basis from the EU US Safe Harbor Agreement.

[8] For example, the EU US Safe Harbor Agreement allows organisations to restrict their self-certification to either online or offline data – but this restriction is not made known to consumers, and does not appear sensible in a modern business environment. A high proportion of Safe Harbor members have made distinctions of this type, without any notice to consumers.

4.2. Benchmark 2 – Usability

Privacy rights should be easy to understand and use for consumers, and easy to manage for business and regulators.

A Global Privacy Standard should promote privacy protection that meets the following criteria:

1. Privacy protection should be easy to understand for consumers. In particular, the use of short form and summary privacy policies should be encouraged and promoted.

2. Privacy protection should be accessible. There should be a focus in privacy documentation on the use of plain language, and measures to ensure that information is accessible for people with relevant disabilities. Information should be provided in multiple languages where appropriate.

3. Privacy protection should not be overly complex or expensive to manage and implement. In particular, complex, costly registration processes that use up scarce funds and resources should be avoided, as they have delivered only minimal benefits to consumers at great cost.[9]

4.3. Benchmark 3 – Access to Dispute Resolution

Protection of privacy rights should be supported by access to affordable and effective dispute resolution.

A Global Privacy Standard should promote privacy protection that meets the following criteria:

1. Privacy protection should include a requirement for organisations to maintain free and fast internal complaints resolution services.

2. Privacy protection should include a requirement for free and fast external complaints resolution services, where complaints are not resolved by the organisation in the first instance. External complaints and complaints made to regulators should include a right of appeal, including a right of appeal on the merits. External complaints services and regulators should be independent and guard against perceptions of bias. Great care should be taken regarding close sponsorship, board memberships and the receipt of fees from organisations who may be the subject of a complaint.

3. Privacy protection should include appropriate back up provisions, allowing the exercise of individual rights and class action rights in the courts where necessary.

4.4. Benchmark 4 – Meaningful Enforcement

Protection of privacy rights requires the presence and appropriate use of meaningful enforcement powers.

A Global Privacy Standard should promote privacy protection that meets the following criteria:

[9] Jurisdictions that have implemented privacy legislation more recently have tended to exclude costly registration processes. See Connolly C, *Asia-Pacific Region at the Privacy Crossroads*, (2008) World Data Protection Report 9(8), pages 8-16. Also, see the discussion in China on the potential exclusion of registration requirements in their draft privacy legislation in Sutton G, Xinbao Z, Hart T, *Personal Data Protection in Europe and China: What lessons to be Learned?*, EU-China Information Society Project, November 2007.

1. Privacy protection should include appropriate enforcement powers for regulators, with sufficient strength to act as a deterrent to organisations.

2. Privacy protection should include a commitment by regulators to actually use these enforcement powers in appropriate circumstances. There may be a general discretion for regulators to conciliate disputes and issue warnings, but they must ultimately be willing to use enforcement powers for serious or repeat infringements of privacy rights.

3. Privacy protection should include the ability for individuals and regulators to *prevent* harm, for example through seeking injunctions or issuing compliance notices. Injunctions and compliance notices are particularly useful in the privacy arena, as they may assist in preventing harm. Once personal information is disclosed it can be difficult to repair the damage using other sanctions and remedies.

4. Privacy protection should include a hierarchy of sanctions and remedies, so that sanctions and remedies can be used that are appropriate for the harm suffered. Sanctions and remedies may include an apology, deletion of data, correction of data, corrective advertising, changes to policies and procedures, remedial training, financial compensation, fines, publication etc.

5. Privacy protection should include the right for an aggrieved individual to seek a determination by a regulator, including the publication of written reasons for the regulator's decision.[10]

6. Protection of privacy rights requires transparency of enforcement, in the interests both of complainants and those being regulated, and to effect the behaviour of both. Transparency requires the statistical reporting of complaints and the regular publication of case studies. Serious complaints should always be the subject of a public report.[11]

4.5. Benchmark 5 – Civil Society Input

Protection of privacy rights requires input from key stakeholders. Government and business stakeholders tend to be well represented in the development of privacy initiatives – Civil Society input is essential to produce a balanced outcome.

A Global Privacy Standard should promote privacy protection that meets the following criteria:

1. Privacy protection should include Civil Society input for all high level global, regional and national privacy standards and frameworks.

2. Privacy protection should include Civil Society input for the detailed development and implementation of privacy laws, and the terms of reference for complaint schemes and regulators, at the national level.

3. Privacy protection should include Civil Society input for all reviews and law reform processes relevant to privacy.

[10] This requirement is intended to address a weakness in many jurisdictions where the regulator can choose not to investigate a complaint, with no further recourse for the complainant.

[11] For more detailed discussion of transparency, see: Greenleaf G, *Reporting Privacy Complaints* (2002) Privacy Law and Policy Reporter 41-48, 74-79 and 111-115. Professor Greenleaf has proposed that Transparency of Enforcement should be developed as a stand-alone benchmark.

4.6. Benchmark 6 – Effective Oversight and Review

Protection of privacy rights requires ongoing oversight and review.

A Global Privacy Standard should promote privacy protection that meets the following criteria:

1. Privacy protection should include oversight by an independent supervisory authority (or authorities)

2. Privacy protection should include monitoring of implementation of privacy rights and the adequacy of their enforcement A process of constant learning and improvement is required in order to provide effective privacy protection.

3. Privacy protection should include regular reviews and guidance in order to accommodate changes in technology, practice and community expectations.

4. Privacy protection should include monitoring to protect against false and misleading claims of privacy protection by organisations.[12]

4.7. Benchmark 7 – International Cooperation

Protection of privacy rights should be international, with support and collaboration amongst nations.

A Global Privacy Standard should promote privacy protection that meets the following criteria:

1. Privacy protection should include provisions that protect information when it is transferred to another jurisdiction.

2. Privacy protection should include guidance on those jurisdictions that meet a test of 'adequate' privacy protection. These lists can be maintained at the international, regional and national level. These lists can improve on the current EU model by allowing partial adequacy (for example, finding that a jurisdiction provides adequate protection for a particular type of data, such as human resources data).

3. Privacy protection should include international guidance on terms that can be included in contracts in order to protect information that is transferred between jurisdictions.[13]

4. Privacy protection should include international cooperation regarding complaints handling and enforcement.[14]

---

[12] See Connolly C, *The US Safe Harbor – Fact or Fiction?* (2008) Privacy Laws and Business International 96, pages 1, 3, 26-27; Connolly C, *Privacy Trustmarks – don't be fooled*, (2009) Privacy Law and Business International 98, pages 9-12.

[13] See, for example, European Commission, *Commission Decision of 27 December 2001 on standard contractual clauses for the transfer of personal data to processors established in third countries, under Directive 95/46/EC*, Official Journal L 6/52, 10 January 2002, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:006:0052:0062:EN:PDF>; see also Office of the Victorian Privacy Commissioner, *Model Terms for Transborder Data Flows of Personal Information*, June 2006, <http://www.privacy.vic.gov.au/privacy/web.nsf/content/guidelines>.

[14] Organisation for Economic Cooperation and Development, *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, 2007, <http://www.oecd.org/dataoecd/43/28/38770483.pdf>.

5. Privacy protection should include support for countries that are developing privacy laws and regulations, including the exchange of skills and information and the provision of training and mentoring.

5. Comparison of current global initiatives

The following table attempts to provide a comparison of three current global privacy initiatives against the Benchmarks proposed in this article. The table provides useful information, despite some limitations in the availability of data.[15]

The full details of the *Joint Proposal for a Draft International Standard on the Protection of Privacy* (the Data Protection Commissioners Standard) have not yet been released. Also, some aspects of the APEC Privacy Framework are incomplete (e.g. the proposed Cross Border Privacy Rules).

Benchmark	CoE Convention (with additional protocol)	APEC Privacy Framework	(Draft) Data Protection Commissioners Standard
Benchmark 1 – Comprehensive Coverage Protection of privacy rights should be comprehensive, with as few gaps and exceptions as possible			
1.1 Applies to all organisations	Yes	No	Yes
1.2 Applies to all sectors	Yes	No	Yes
1.3 Applies to all consumers	Yes	Yes	Yes
1.4 Minimised exemptions	Yes	No	Yes
1.5 Applies to all data formats and forms of communication	Yes (although scope can be limited by declarations)	Yes	Yes
Benchmark 2 – Usability Privacy rights should be easy to understand and use for consumers, and easy to manage for business and regulators.			
2.1 Easy to understand; short form	No	Encouraged	Encouraged
2.2 Accessibility	No	Yes	Yes
2.3 Low complexity; low cost	Registration requirements are discretionary	No – highly complex, expensive implementation based on CBPRs and registration	Registration requirements are discretionary
Benchmark 3 – Access to Dispute Resolution Protection of privacy rights should be supported by access to affordable and effective dispute resolution			
3.1 Requirement for free and fast internal dispute resolution	No	Limited	No
3.2 Requirement for free, fast, and independent external dispute resolution	No	Limited	No
3.3 Allows exercise of individual rights, court action, and other 'backup provisions'	Yes	No	Yes

[15] The analysis contained in the table represents the personal views of the author. Comments are welcome.

Benchmark	CoE Convention (with additional protocol)	APEC Privacy Framework	(Draft) Data Protection Commissioners Standard
Benchmark 4 – Meaningful Enforcement Protection of privacy rights requires the presence and appropriate use of meaningful enforcement powers.			
4.1 Appropriate enforcement powers for regulators	Yes	No – choice of enforcement method includes self regulation	Yes
4.2 Commitment by regulators to use enforcement powers	Yes	No	Yes
4.3 Ability for individuals to seek injunctions	No	No	Unknown
4.4 Extensive list of sanctions and remedies	Limited	No	Yes
4.5 Right to seek determination by regulator, including written reasons for decision	Yes	No	Yes
4.6 Transparency of enforcement	Limited	Limited	Unknown
Benchmark 5 – Civil Society Input Protection of privacy rights requires input from key stakeholders. Government and business stakeholders tend to be well represented in the development of privacy initiatives – Civil Society input is essential to produce a balanced outcome.			
5.1 Civil Society input for high level global, regional and national privacy standards and frameworks	Yes	No – Civil Society excluded from early development and not granted same input status as business groups	Limited
5.2 Civil Society input for detailed development and implementation of laws and terms of reference for regulators and complaint schemes	Yes	No	Limited
5.3 Civil Society input for relevant reviews and law reform processes	Yes	No	Limited
Benchmark 6 – Effective Oversight and Review Protection of privacy rights requires ongoing oversight and review.			
6.1 independent supervisory authority	Yes	No	Yes
6.2 Monitoring of implementation and enforcement	Yes	Limited – requirement for country reports.	Yes
6.3 Regular reviews and guidance	Yes	Unknown	Unknown
6.4 Monitoring for false claims of privacy protection by organisations	n/a	No – claims of APEC compliance already widespread with no central control	n/a
Benchmark 7 – International Cooperation Protection of privacy rights should be international, with support and collaboration amongst nations.			
7.1 Protection of information transferred to another jurisdiction	Yes	Limited	Yes
7.2 Guidance on 'adequacy' of protections in jurisdictions	Yes	No	Yes
7.3 International guidance on contract terms for privacy protection	Yes	No	Yes

Benchmark	CoE Convention (with additional protocol)	APEC Privacy Framework	(Draft) Data Protection Commissioners Standard
7.4 International cooperation on complaints and enforcement	Yes	Yes – encouraging progress on cross-border cooperation – key agreements still in development	Yes
7.5 Support for countries developing privacy protection; exchanging skills and information and training	No	Yes	Unknown