'Modernising' Data Protection Convention 108: A Safe Basis for a Global Privacy Treaty?

Graham Greenleaf
University of New South Wales

Follow this and additional works at: http://law.bepress.com/unswwps-flrps13

Part of the Comparative and Foreign Law Commons, Computer Law Commons, International Law Commons, Internet Law Commons, and the Law and Society Commons

Recommended Citation
http://law.bepress.com/unswwps-flrps13/34

This Article is brought to you for free and open access by the University of New South Wales Faculty of Law Research Series at bepress Legal Repository. It has been accepted for inclusion in University of New South Wales Faculty of Law Research Series 2013 by an authorized administrator of bepress Legal Repository.
‘Modernising’ data protection Convention 108: A safe basis for a global privacy treaty?

Graham Greenleaf, Professor of Law & Information Systems, University of New South Wales*

8 May 2013 – Accepted for publication by Computer Law & Security Review, Vol 29, Issue 4, forthcoming, July/August 2013. Comments to <graham@austlii.edu.au> are invited. The published version should be cited.

Contents

‘Modernisation’ and ‘globalisation’ of Convention 108: A symbiotic relationship ....................... 2
Obligations of the parties ................................................................................................................. 3
Data protection standards ............................................................................................................... 4
Additional obligations ................................................................................................................... 5
Domestic enforcement mechanisms required .............................................................................. 5
New roles for the Convention Committee .................................................................................. 5
Accession by non-European states ............................................................................................ 6
Evaluating accession candidates and the performance of Parties ............................................. 7
Ratification: A new twist ............................................................................................................... 7
Data export restrictions: Why is adequate not appropriate? ....................................................... 7
Data exports ‘safeguards’ and exemptions: How safe are they? .................................................. 9
The present danger: ‘Interoperability’ across the species barrier ............................................. 10
Will a modernised Convention pass the Goldilocks test? ....................................................... 11

*Acknowledgment is made of valuable comments received from Sophie Kwasny and Marie Georges, but responsibility for all content and opinions in this article remains solely with the author.
‘Modernisation’ and ‘globalisation’ of Convention 108: A symbiotic relationship

The Consultative Committee of Council of Europe data protection Convention 108\(^1\) adopted its final proposals\(^2\) for ‘modernisation’ of the Convention in November 2012,\(^3\) for transmission to the Committee of Ministers for adoption. They are to be finalised by an ad-hoc committee of the Committee of Ministers\(^4\), and may be amended there or by the Committee as a whole, so how ‘final’ they are remains to be seen. A draft Explanatory Report, to be prepared by the Convention 108 Bureau, is not yet available publicly, but was to be finalised and circulated for consideration at the Bureau’s meeting at the end of May 2013\(^5\). It may clarify or resolve some of the issues raised in this article.

The ‘globalisation’ of Convention 108 (developing it into a global data privacy agreement, open to all countries providing the required level of data protection) is also now underway,\(^6\) and Uruguay has become the first non-European state to become a Party to the Convention.

The advantages of ‘globalisation’ are significant for both existing parties and new entrants,\(^7\) but these advantages depend upon the Convention requiring a sufficiently high level of privacy protection for non-European accessions (including restrictions on data exports to recipients in states not parties to the convention), and requiring that these protections continue to be provided in practice. This article argues that, in relation to both of these requirements, adoption of the ‘modernisation’ proposals will make ‘globalisation’ work better for everyone, provided the data export restriction issue is resolved somewhat better than currently proposed.

Some general observations can be made about the proposals. First, many changes will have the effect of making the ‘globalisation’ of Convention 108 more effective, both in terms of the procedures for accession of new members, and in providing post-accession mechanisms to ensure that the Convention is in fact being complied with by the parties to it. This is particularly so with the provisions that in effect absorb the Additional Protocol into the Convention (requiring a data protection authority, data export restrictions, and access to the courts), so that it is not possible to accede to one without the other. Second, some aspects of the proposals will help the Convention ‘keep pace’ with stronger provisions likely to be included in the proposed EU Regulation. Third, it will become more clear that the standards

---

\(^1\) Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, ETS No. 108


\(^3\) Convention 108 Consultative Committee (T-PD) 29th plenary meeting Strasbourg 27 - 30 November 2012, Abridged Report, item 2 states that the T-PD ‘gave a third reading to the proposals for modification of Convention 108, revised by its Bureau following the 28th plenary meeting, and adopted those proposals for transmission to the Committee of Ministers (set out in Appendix 3), and invited the Committee of Ministers to entrust the finalisation of the proposals to an ad hoc committee, instructing its Bureau to finalise the draft explanatory report in the light of the discussions’

\(^4\) To be called the Ad-Hoc Committee on Data Protection (CAHDATA), and to include observers from numerous international organisations – see item 3, Convention 108 Bureau (T-PD-BU) 29th meeting of the Bureau 5-7 February 2013 Abridged Report Strasbourg, T-PD-BUR(2013)RAP29Abr

\(^5\) Ibid, Item 2


required for a non-European country to accede to the Convention differ from those by which the EU assesses the ‘adequacy’ of a non-EU country’s data protection provisions, but on the other hand it is not clear whether a suitable substitute has been found for ‘adequacy’ as the standard to measure data export restrictions.

This article analyses the significance of the proposed ‘modernisation’ changes, comparing them where needed to the previous proposals under consideration in March 2012, and whether the final proposals are a sound basis for a global data protection treaty. The less controversial aspects of the proposals are first considered, saving for last that hardy perennial of contention, data export restrictions, which necessarily overshadows other considerations. Finally, the question is asked of whether a modernised Convention would pass the Goldilocks Test? References to Articles of the Convention are, unless stated otherwise, to the Article numbers in the final proposals.

**Obligations of the parties**

Parties must apply their data protection laws to ‘every individual subject to the jurisdiction of the Parties, whatever their nationality or residence’ (A 1). Restricting protection to citizens is not permitted. A party must ‘apply this Convention to data processing subject to its jurisdiction’ (implying all data processing), with the exception of ‘data processing carried out by a natural person for the exercise of purely personal or household activities’ (A 3).

The Convention states that its primary role is as a human rights instrument (A 1). ‘Each Party shall take the necessary measures in its domestic law to give effect to the provisions set out in this Convention and ensure their effective application’ (A 4(1)). This means that the requirement for both compliance with the Convention, and accession to it, is simply that a party’s domestic law and practice must show full compliance with all its terms (though of course there is always some leeway as to what counts as full compliance). The wording is different from the existing Convention, but the effect is the same. These measures must be taken ‘prior to ratification or accession’ (A 4(2)), not only prior to entry in force as at present (which is three months after ratification). This closes a loophole where a State could in theory ratify without having brought all necessary measures into effect.

Most important, a Party ‘undertakes to allow the Convention Committee … to evaluate the observance of its engagements and to contribute actively to this evaluation, notably by submitting reports on the measures it has taken and which give effect to the [Convention] provisions’ (A 4(3)). What this probably means (but this will need to be confirmed in the Explanatory Report) is that Parties will have to show that they ‘give effect’ to Convention requirements as a matter of practice, and not merely as a matter of passage of legislation. In the context of EU ‘adequacy’ determinations, terminology such as ‘a good level of compliance’, ‘provision of appropriate redress’ and ‘provision of support and help’ are used to indicate the substantive effect that is required.

No reservations from Convention provisions are allowed (A 25). It applies to all personal data. Some derogations from some of the data protection standards by domestic legislation are allowed (A 9), somewhat more narrowly defined than in the existing Convention.

---

Data protection standards

The existing Convention’s data protection standards are in Articles 5-9\(^9\) which set them out in ‘broad brush fashion’\(^{10}\). In the proposed ‘modernised’ Convention they are also in Articles 5-9. As now, they are minimum standards, and Parties may choose to provide stronger protection (A 11).

There are two new general requirements for processing in Article 5:

1. Data processing shall be proportionate in relation to the legitimate purpose pursued and reflect at all stages of the processing a fair balance between all interests concerned, be they public or private interests, and the rights and freedoms at stake.

2. Each Party shall provide that data processing can be carried out on the basis of the free, specific, informed and [explicit, unambiguous]\(^{11}\) consent of the data subject or of some legitimate basis laid down by law.

Requiring proportionality at all stages of processing is a notable improvement. Article 5(3) is much the same as the processing principles in the current Article 5, including the existing weak restriction on secondary use (‘not processed for incompatible purposes’). However, collection and processing of personal data is now limited by the higher EU standard of the ‘minimum necessary’ rather than ‘not excessive’.

The categories of sensitive data which must have additional ‘appropriate’ safeguards (particularly against discrimination) are expanded to include genetic data, identifying biometric data, and trade union membership (A 6). ‘Appropriate’ is undefined, but that does not matter here, because the protections of sensitive data are additional to (reinforcing) the base standards.

The security principles has had added to a requirement of notification, ‘without delay’ to the supervisory authorities ‘of those data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects’ (A 7), but there is no requirement to notify the data subject.

A new Article 7bis (‘Transparency of processing’) provides previously missing requirements of notification to data subjects of various matters at the time of collection. They will also apply when the personal data is collected from third parties, except where the processing is ‘expressly prescribed by law’ or notification ‘proves to be impossible or involves disproportionate efforts’ (A 7bis(2)).

Article 8 expands the existing rights of the data subject in various ways which better align the Convention with the EU Directive (and proposed Regulation), including rights: to have their

\[^{9}\] Most of the data protection content in the existing Convention comes from Article 5 (Quality of data) which requires that: ‘Personal data undergoing automatic processing shall be: 1. obtained and processed fairly and lawfully; 2. stored for specified and legitimate purposes and not used in a way incompatible with those purposes; 3. adequate, relevant and not excessive in relation to the purposes for which they are stored; 4. accurate and, where necessary, kept up to date; 5. preserved in a form which permits identification of the data subjects for no longer than is required for the purpose for which those data are stored’. Other than that, there are familiar principles requiring ‘appropriate’ data security (Article 7), and rights to ascertain the existence of personal files, to access them, and to correct them (Article 8). There is also a provision for ‘sensitive’ data in Article 6 ‘Personal data revealing racial origin, political opinions or religious or other beliefs, as well as personal data concerning health or sexual life [or criminal convictions], may not be processed automatically unless domestic law provides appropriate safeguards.’


\[^{11}\] Sets of terms in brackets mean that the Consultative Committee did not agree on which was the preferable term.
views considered before decisions are made on the basis of automated processing; to object to processing; to know on request ‘the reasoning underlying the data processing’ applying to them; and to benefit from assistance of a supervisory authority no matter where they reside.

**Additional obligations**

A new Article 8bis goes further, building into the Convention protections similar to those expected to be included in the EU Regulation, which require the controller, or where applicable the processor:

1- to take ‘all appropriate measures to implement’ the principles and obligations and ‘to establish internal mechanisms to verify and be able to demonstrate at least to the supervisory authorities’ compliance with the applicable law (an ‘accountability’ principle);

2- to carry out a risk analysis of the potential impact of the intended data processing on the rights and fundamental freedoms of the data subject and design data processing operations in such a way as to prevent or at least minimise the risk of interference with them (a ‘privacy by design’ and ‘privacy by default’ principle);

3- to design products and services to take into account the implications of the right to the protection of personal data and facilitate compliance of processing with applicable law (a ‘privacy by design’ principle);

4- to adapt the previous requirements, according to the size of the controller or processor, the volume or nature of data processed and, more generally, in light of the risks for the interests, rights and fundamental freedoms of the data subjects.

The data protection Principles proposed for the revised Convention are therefore very considerably stronger than those in the OECD Guidelines, and may end up being comparable to those in the proposed EU Regulation (although it is too early to be sure of that).

**Domestic enforcement mechanisms required**

Article 12 bis inserts into the Convention the requirements previously in the Additional Protocol for Supervisory Authorities (with a right of appeal against their decisions to the courts). It adds stronger requirements and functions involving obligations to ensure transparency of their activities; mandatory powers to make decisions concerning Convention obligations, including sanctioning administrative offences; requirements they be consulted on legislative and administrative changes; and the function of ‘approval of standardised safeguards’ concerning data exports. There are also detailed provisions requiring cooperation between supervisory authorities (Articles 13–17), valuable when complaints may involve acts occurring within the jurisdiction of more than one Party.

Article 10 now requires appropriate ‘judicial and non-judicial’ sanctions and remedies for violations. The Explanatory Report to the existing Convention (para 60) mentions ‘civil, administrative, criminal’ sanctions, the choice of which should be left to each State. Article 10 now adds that these sanctions should be both ‘judicial and non-judicial’, implying that both the courts and non-judicial bodies should be able to issue sanctions. However, it does not go so far as requiring that data subjects have a direct right to sue in a civil action in Court for breaches.

**New roles for the Convention Committee**

The Consultative Committee is to be re-named the Convention Committee, and its functions expanded and strengthened (A 19), including the following new powers:
Final proposals for ‘modernising’ data protection Convention 108

(a) may express an opinion on any question concerning the interpretation or application of this Convention [no longer requiring the request of a Party];
(b) shall prepare, before any new accession to the Convention, an opinion for the Committee of Ministers relating to the level of data protection of the candidate for accession;
(c) may, at the request of a State or an international organisation or on its own initiative, evaluate whether the level of data protection the former provides is in compliance with the provisions of this Convention;
(d) may develop or approve models of standardised safeguards referred to in Article 12;
(e) shall periodically review the implementation of this Convention by the Parties in accordance with the provisions of Article 4.3 and decide upon measures to take where a Party is not in compliance with the Convention;
(f) shall facilitate, where necessary, the friendly settlement of all difficulties related to the application of this Convention.

These functions are very significant, and could give the Committee a role of similar importance to the Article 29 Working Party under the EU Directive. The big difference is of course that this is not a committee made up of Data Protection Commissioners, but one comprised of State representatives (but they are often drawn from data protection authorities). How energetic will they be in exercising the above powers to ensure that other States which are parties to the Convention (or applying to so become) are fully protecting the rights of data subjects as required by the Convention? It is not a question to which an a priori answer can be given.

The Committee also now has the ability to invite observers to its meeting by a two-thirds majority of members entitled to vote, rather than requiring unanimity (A 18(3)). The input from these non-State observers is likely to help ensure that problems with the Convention’s operation are brought to the attention of the Committee, and that they find it difficult to ignore them.

Accession by non-European states

The provisions concerning accession by States not members of the Council of Europe (A 23) is only changed by addition of a requirement that the Committee of Ministers is only to invite accessions ‘after consulting the Parties to the Convention and obtaining their unanimous agreement and in light of the opinion prepared by the Convention Committee in accordance with Article 19.e.’ The requirement to consider (but not necessarily to follow) the opinion of the Convention Committee reflects current practice adopted in the two non-European accession invitations to date. The reference to the unanimous agreement of the parties means that non-European Parties (such as Uruguay and Morocco are soon likely to become) will have the same powers of veto in relation to other new memberships as Council of Europe member States have already. It is possible for States to accede in relation to only part of their territory (A 24(1)). For example, if China wished to accede in relation to the Hong Kong SAR only, it could do so after ‘modernisation’12.

It is also intended that the ad hoc committee of member States (CAHDATA) which is to finalise the ‘modernisation’ of Convention 108 is to include ‘as observers, an extensive list of non-member states and certain international organisations (United Nations, Organization of American States, African Union, Economic Community of West African States, Association of

12 Even though the People’s Republic of China can allow Hong Kong to accede to some international agreements, Convention 108 is only open to States (A 23) at present.
Southeast Asian Nations, [and] APEC.’ It seems, therefore, that part of the CoE’s strategy for ‘globalisation’ is to engage significant regional organisations in the process of ‘modernisation’ of the Convention, as well as individual States that may have an interest in accession.

**Evaluating accession candidates and the performance of Parties**

In anticipation of the adoption of the proposals, the Consultative Committee has put forward for discussion a proposal for largely similar procedures for both the evaluation of candidates for access and for periodic evaluations of all Parties’ compliance with the Convention, and the measures that should be taken in event of non-compliance.14

The evaluations would be carried out by a committee of probably six members of the Consultative Committee, with a mix of government and supervisory authority members, with geographic balance, and a partial rotation of members over six year terms. In both cases, the legislation in force, the supervisory authority, and the remedies available to data subjects would be examined. Both questionnaires and in-person visits would be used. An open process is proposed (very different from EU ‘adequacy’ evaluations) which would involve dialogues with the candidates/Parties that would involve interested NGOs, and production of a draft opinion, and final opinion for comment by the candidate/Party. Both the final opinion and the comments would be made public after transmission to the Convention Committee. Such openness would increase confidence in the quality of the Convention and its processes.

In the event of finding non-compliance, the Convention Committee would aim to assist the relevant government and supervisory authority to draw up a plans to deal with the deficiencies, and report on progress. This is not unusual with treaty bodies, as there are usually no powers to take other enforcement actions. In this respect, it is unlike the power of the European Commission to take recalcitrant governments before the European Court of Justice in relation to the data protection Directive.

**Ratification: A new twist**

While the new Convention (technically, a Protocol to the existing Convention) requires ratification by all existing Parties, this is only so in theory. This is because the proposals have a ‘silence implied consent’ clause which provides that, unless all Parties give positive consent, the Protocol ‘shall enter into force following the expiry of a period of [two] years after the date on which it has been opened to signature, unless a Party to the Convention has notified the Secretary General of the Council of Europe of an objection to its entry into force’ (Article un-numbered). It would then only enter into force when the objecting Party ratifies the Protocol.

**Data export restrictions: Why is adequate not appropriate?**

The guarantee of free flow of personal data between parties to the Convention (A 12(1)) is only justifiable if it is coupled with an obligation on parties not to export personal data to organisations in States that are not parties unless the protection of privacy continues to be guaranteed despite the data export. This is the basic principle of balancing free flow of personal data with data export restrictions. A year ago, there were deep differences within the

---


14 Consultative Committee Information Elements on the Evaluation and Follow-up Mechanism, Strasbourg, 29 January 2013, T-PD-BUR(2013)02
Consultative Committee about how to define the required data export restrictions, and competing proposals.\textsuperscript{15} The final proposals seem to be a reasonable compromise in some respects, but in other respects as are so ill-defined that they are dangerous for data subjects unless they receive clarification.

The Additional Protocol to the existing Convention requires that data exports (‘transfers’) can only be allowed if ‘an adequate level of protection’ is provided, and the explanation of this is in very similar terms to ‘adequacy’ in the context of the EU data protection Directive. In 2012 the Consultative Committee was sticking to ‘adequacy’ as the touchstone for export limitations:\textsuperscript{16}

The proposed provisions are still based on the well-known notion of an “adequate level of protection”. The Convention shall continue to require such protection, in particular if data is communicated or disclosed to recipients not subject to the jurisdiction of a Party to the Convention, recognising that this rule has promoted the development of data protection laws around the world.

However, the final proposals refer instead to ‘an appropriate level of personal data protection based on the principles of the Convention’ (A 12(2)). This ‘appropriate’ protection can be provided by a country’s domestic law (and international commitments) and can also be provided by various forms of ‘safeguards’ (discussed later) (A 12(3)(b)). ‘Appropriate’ protection does not mean that all ‘principles of the Convention’ must be observed, otherwise Article 12(2) would say so. What ‘an appropriate level’ of protection requires in a country’s domestic law, or in the ‘safeguards’, could be clarified to some extent by the Explanatory Report, but whether it will be is uncertain.

The danger of such non-explanation is that ‘appropriate’ has little or no meaning in the history of data protection. On the other hand, ‘adequate’ has a known and reasonably strong meaning that has developed over nearly 20 years. ‘Adequacy’ is a term and a concept that has been disliked by some countries in various forums over the years, but without access to the minutes of the Consultative Committee discussions, it is not helpful to speculate which Parties or Observers led the Consultative Committee to abandon ‘adequacy’. In the longer term, the meaning of ‘appropriate’ will be a question of interpretation of the Convention on which the Convention Committee will be entitled to give opinions (A 19(d)), but its opinions are not binding. There are no final judicial arbiters of the meaning of such terms.\textsuperscript{17} Disputes about the meaning of Convention 108 can only be settled by diplomacy, not by a Court. That is why the meaning of key terms must be reasonably clear on the face of the Convention itself, or at the very least in the Explanatory Report accompanying the Convention. Such replacement of key meaningful terms by terms whose meanings are more easily contestable is common in multilateral trade and intellectual property negotiations,\textsuperscript{18} and indicates the need for careful and sceptical consideration of such changes in terminology in data protection agreements.

‘Adequate’ may not be the perfect term, but its retention would pose much less risk to the interests of data subjects, and would keep Convention 108 better aligned to both the EU

\textsuperscript{15} See ‘Data export restrictions remain contentious’ in Greenleaf ‘Scope remains to further strengthen Council of Europe data privacy Convention 108’ (above).

\textsuperscript{16} As above.

\textsuperscript{17} Citizens of European countries may be able to take the same issues to the European Court of Human Rights under Article 8, though not formally invoking the Convention. The same may apply to regional human rights courts in Latin America.

\textsuperscript{18} For discussion of the politics of such negotiations, see P Drahos and J Braithwaite \textit{Information Feudalism}, Earthscan, London 2002
Directive and its successor Regulation, where retention of ‘adequacy’ as the key term is proposed\(^{19}\). ‘Equivalent’ protection, or protection ‘of similar effect’, are other terms which are meaningful, and connote a standard not of being identical but functionally equivalent. ‘Appropriate’, in contrast, is meaningless by itself, even when ‘based on the principles of the Convention’. To see this, just ask the question ‘what would the US State Department think is appropriate?’

For anyone whose main interest is strong data protection standards, such as civil society organisations, Article 12 is the key provision of the Convention. If it is faulty, this cannot be compensated for by otherwise strong provisions, because accession would then mean a commitment to export personal data to places which offer low protection.

A special exception has been added to the obligation of free flow of personal data between Parties, in order to accommodate the position of EU member States and their need to comply with the EU data protection Directive. EU States may restrict data exports to other Parties to the Convention unless those data exports comply with Article 12(3)(b) ‘ad hoc or approved standardised safeguards’ (proviso to A 12(1)). Claims that a country’s domestic legislation is ‘appropriate’ are not sufficient. The reasoning behind this is presumably that the EU member State’s data protection authority can veto any ad hoc safeguards that do not meet EU requirements, by Article 26 of the Directive, and that ‘standardised safeguards’ will meet the EU requirements. This convoluted provision might not be needed if the Convention also used ‘adequacy’ as its terminology.

**Data exports ‘safeguards’ and exemptions: How safe are they?**

‘Appropriate’ protection can also be provided by ‘ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by the persons involved in the transfer and further processing’ (A 12(3)(b)). ‘Standardised’ safeguards must be approved by a State’s Supervisory Authority (A 12bis(2)(b)). The Convention Committee may ‘develop or approve models of standardised safeguards’ (A 19(d)), but cannot mandate uniform safeguards. Where such standardised safeguards exist, approval of data exports in individual transactions by the Supervisory Authority is not required if they are complied with.

Each Party may provide for further exceptions allowing data exports in three situations (A 12(4)):  

(a) ‘the data subject has given his/her specific, free and [explicit, unambiguous] consent, after being informed of risks arising in the absence of appropriate safeguards’, or  
(b) ‘the specific interests of the data subject require it in the particular case’, or  
(c) ‘prevailing legitimate interests, in particular important public interests, are provided by law and constitute a necessary measure in a democratic society’.\(^{20}\)

It is important to note that these three exceptions are neither compulsory nor automatic, but depend upon domestic enactment by parties, and may be subject to any additional conditions those enactments may impose, but may not be any broader than specified by Article 12(4). However, within the limits of Article 12(4), States may make exceptions which apply to

\(^{19}\) See European Commission Proposal for a Regulation Of The European Parliament and of The Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final, Brussels, 25.1.2012, particularly Articles 25(2), 41 (passim), and 45(2)

\(^{20}\) This is reiterated in a somewhat redundant provision in Article 9(2), allowing restrictions on Article 12 ‘where they are provided by law and constitute a necessary measure in a democratic society for the freedom of expression.’
classes of data subjects of unlimited breadth, may involved very broad descriptions of the relevant interests, do not necessarily impose any duties of care (or even stronger liabilities) on the exporter, or necessarily require any minimal protections to be provided by the importer. If misused by States, thought over-broad legislation or regulations, they could result in massive flows of personal data being allowed to jurisdictions offering little or no data protection. These exceptions are over-broad, are a risk to data subjects, and possibly might not be consistent with the data export laws of some countries considering accession to Convention 108.

What guarantees must be provided that the ad hoc ‘safeguards’ required under (3)(b) actually exist, or that the conditions for exemptions required by (4)(b) or (c) are actually satisfied? The protection of the data subject depends entirely on such guarantees, otherwise companies will simply export personal information wherever they want, while pretending to comply with these provisions and obtaining a fig leaf of legitimacy. Article 12(5) provides that:

> Each Party shall provide that the competent supervisory authority ... [must] be informed of the modalities regulating the transfers of data provided for in paragraphs 3.b when ad hoc safeguards are set up, 4.b and 4.c. It shall also provide that the supervisory authority be entitled to request that the person who transfers data, or the recipient, demonstrate the quality and effectiveness of actions taken and that the supervisory authority be entitled to prohibit, suspend or subject to condition such transfers of data’

This seems to imply that the supervisory authorities must be informed in advance of any ad hoc measures before data is transferred, but it is unclear whether ex post facto notification of transfers pursuant to (4)(b) or (c) are acceptable. The Explanatory Report (or, better still, the Convention) needs to confirm these matters. In relation to (4)(b) and (c), the authorisation of these exceptions in domestic legislation must also comply with Article 12(5).

It is also unfortunate that clause (3)(b) does not explicitly say ‘enforceable by the data subject’, and that the enforceability is against any party involved in the transfer. If there are non-European parties to Convention 108, particularly from common law countries, it cannot be assumed that contracts for the benefit of data subject will be enforceable by them, because the doctrine of privity of contract may apply.

**The present danger: ‘Interoperability’ across the species barrier**

It is a current strategy of the Obama Administration to demand ‘interoperability’ with and ‘mutual recognition’ for its proposed ‘Framework’ before that initiative has any reality.21 The USA and its allies have been pushing since at least late 201122 for ‘interoperability’ to be recognised as a primary goal, in all international fora, particularly when agreements and standards concerning data protection are being revised. These include in the OECD revisions of its Guidelines and in APEC/EU discussions. There must therefore be great sensitivity to this issue in the forums of the Council of Europe until the modernisation process is complete.

‘Interoperability’ cannot be an end in itself in data protection negotiations, but only a means of reducing formalities through cross-recognition of fully compatible and equivalent standards and mechanisms. Otherwise ‘interoperability’ or ‘mutual recognition’ is just a mask

---


for capitulation to the demand the stronger party. ‘Interoperability’ is only sensible (perhaps even meaningful) between legal instruments of like pedigree. Convention 108 is a binding international agreement. The OECD Guidelines are just that, guidelines, they have no legal effect anywhere. The APEC Framework is the same, there are no APEC ‘rules’, its Framework is a non-binding instrument and APEC is not an international organisation in the normal sense or even a treaty. There cannot be any worthwhile interoperability or ‘mutual recognition’ between legally binding requirements and mere voluntary commitments. APEC’s proposed Cross Border Privacy Rules (CBPR) scheme does not yet have a single country complying with it, and if and when it does its standards will all so far short of the Convention as to be derisory. The Council of Europe must therefore be vigilant to ask what is any interoperability between, and what is the equivalence or similar effect that justifies mutual recognition when considering the (revised) OECD Guidelines and the ‘promises’ of APEC’s CBPR.

Seen in this light, the choice of ‘appropriate’ protection as a standard to replace ‘adequacy’ requires particular care to be taken that it does not accommodate ‘interoperability’ with other supposed data protection standards which will result in abandonment of proper investigation of whether the standard of privacy existing in countries at the other end of the interoperability chain do in fact meet the standards of the Convention. Those who support data protection need to help stiffen European resolve to confront the challenges presented by American pressure to prematurely adopt ‘interoperability’, and the ideologies that drive it.

Will a modernised Convention pass the Goldilocks test?

Putting aside for the moment the question of data exports, the ‘final proposals’ for modernisation of Convention 108 provide a higher but reasonable standard of data protection, as discussed in this article.

While it is beyond the scope of this article to conduct the necessary detailed comparison, it appears that the standard of data protection currently proposed for modernisation of Convention 108 is one that is likely to be largely consistent with the standards which may emerge from the European Union’s development of a new Regulation to replace the existing Directive. This will not be certain until the reforms of both instruments are finalised. But if this largely consistent development occurs, then these two instruments will together constitute a new ‘European standard’ to replace the current standard created jointly by the EU Directive and the current Convention 108 (and Additional Protocol), which has had a dominant effect on the development of national data protection laws around the globe.

However, because of the ‘globalisation’ of Convention 108, if there is a significant increase in non-European accessions, this will mean that countries outside Europe have an increasing influence on the development of this originally European standard, making it more of a global standard in its ‘ownership’ not only its influence.


24 Waters, N ‘US enters APEC Privacy Rules, system, but value for business?’ Privacy Laws & Business International Report, No. 120, December 2012, 19-21

25 The Committee on the Present Danger <http://www.committeeonthepresentdanger.org/> is a US foreign policy advocacy group which states that its mission is ‘to stiffen American resolve to confront the challenge presented by terrorism and the ideologies that drive it.’

But the success of globalisation depends largely on the perceptions of non-European states, and whether they wish to apply to accede to the Convention. The ‘modernised’ Convention will have to pass the Goldilocks Test. Its standards cannot be too ‘hot’: they must not impose data protection standards so high that domestic political opinion will not accept them. But the standards must not be too ‘cold’: they cannot be so low that they will require free flow of personal information to other Parties to the Convention who provide a much lower standard of data protection than they do (but sufficient to allow them to accede); and nor can they allow those parties to re-export personal data to other countries with standards that are too low. The Convention’s standards of data protection must be ‘just right’ to ensure eventual global adoption. At present, we cannot say whether it will be ‘just right’. While modernisation is still cooking, care must be taken that to avoid Convention 108 becoming too cold and unpalatable because of the quest for ‘interoperability’. 