

Cross-border data flows:

Who benefits from abandoning borders?



Graham Greenleaf & Nigel Waters

Let's send your details to Russia

- + UPP 11 now applies to agencies as well as companies
- ∅ No longer any border controls on data transfers, only 'accountability'
 - Never a breach merely because of destination of transfer.
 - Consent to transfer not required before transfer occurs.
 - Not even possible to forbid transfer of your data to anywhere overseas, once it has been collected.
 - **It's always OK to transfer your data to Russia**
 - Or to anywhere else where sending personal data is dangerous to you
 - Subject to compliance with Use & Disclosure principles - including secondary use
- ∅ **Transferors remain liable for UPP breaches ('accountability')**
 - **BUT only if they are foolish enough not to fit under any of 4 exemptions (so 'accountability' will probably never happen)**
- 'Accountability' is inadequate protection in any event
 - ∅ Requires individual to be aware of, and to prove, breach of UPPs in a foreign country before any liability to arise in transferor

Bottom line: Better to make transfer a breach in itself (ie 'border controls'), unless an justifiable exemption from liability applies

How to avoid 'accountability' for Russian transfers

How justifiable are the ALRC's proposed exemptions from liability?

- 1 Exempt from liability if on a Government-published Whitelist.
 - Inadequate guarantees on objectivity of Whitelist
 - ∅ OPC to have no role in development of Whitelist
 - ∅ Not even a legislative instrument - No Parliamentary oversight
 - ∅ Result is that whole thing is political, and privacy will lose
- 2 Exempt from liability if you transfer to a country you '**reasonably believe**' to have 'protections substantially similar to the model UPPs'.
 - ∅ 'Reasonable belief' is easily manipulated: Just hire a pliable consultant to inform your belief. Black can become White.
 - **Objective test needed**: are the protections in fact substantially similar?
 - ∅ Ambiguous?: 'Effectively upholds privacy protections' implies remedies, not only principles, but 'substantially similar *to these principles*' undermines that. Should say 'to this Act' to remove doubt.

More exemptions from liability

- 3 Exemption if authorised or required by law (UPP 11(1)(c)).
 - ∅ Preferable if only where required by law
- 4 Exemption if notice given of 'no liability for transfer' (UPP 11(1)((b)))
 - Only applies after express advice that transferor will no longer be liable (b).
 - + Notice of 'no liability' may serve to prevent some unwise consents
 - ∅ But consent is likely to be illusory - ALRC failed to deal with bundled consent, which can include consent to overseas transfers.
 - ∅ ALRC does not require this notification to state the proposed destination
 - Informing individuals of overseas transfers - but it is inadequate
 - + Privacy Policy has to say whether PI may be transferred outside Australia, and to list which countries it will go to (Good – helpful perhaps with SWIFT).
 - ∅ BUT the UPP 11(1)((b)) notice given to individuals, where this would be far more use, is not required to state this.
 - ∅ **Result is very poor:** a Privacy Policy need not distinguish between different PI collected, but a Notice should relate to specific PI collected.

Ø Borders abandoned

Border posts abandoned, but with no countervailing benefits to consumers/citizens

Accountability is no substitute unless it applies in all cases except transfers required by law or with much stronger requirements for fully informed, and non-bundled consent than are currently proposed.

CoE Conv 108 standards

- What standard does CoE Convention 108 require?
 - Consultative Committee may advise Council of Ministers (A 19, 20) whether non-European countries meet Conv 108 requirements (uncertain as yet)
 - Principles are similar to those of OECD Guidelines
 - Enforcement and mutual assistance requirements are modest
- Additional Protocol (ETS No 181) adds complications
 - 20/40 parties to Conv. 108 have acceded; 14 more have signed
 - Requires legislation and an independent authority (Conv 108 does not)
 - Requires data export limitations (Conv 108 does not)
- Which non-European countries could meet CoE accession requirements?
 - Arguable that Australia and NZ could accede to both Convention and Additional Protocol
 - Arguable that South Korea, Japan and Taiwan could accede to Convention
 - Potentially, Canada, some Latin American, and some Middle East countries

Bottom Line: Considerable scope for non-European accessions

Potential for CoE Conv 108 adoption in Asia-Pacific

- Potential advantages
 - Not inconsistent with APEC obligations
 - Joining a Convention is voluntary, not an external imposition
 - Would result in free flow of PI to and from signatory non-EU countries (A 12(2) requires)
 - Would result in free flow of PI to and from EU countries, *unless* they specifically derogate against exports to a country (A 12(3)(b))
 - Would encourage other Asia-Pacific countries to develop their laws and enforcement to CoE standard, to gain the benefits of accession
- Potential disadvantages
 - Civil Society view may be that Conv. 108 standards are too low
 - Might it require exports to countries whose laws are not strong enough?
 - No mechanism to require acceding countries to adhere to standards

Bottom Line: Deserves considerable further study by all Asia-Pacific countries with data protection laws; May be a path to a global agreement, avoiding some problems of EU 'adequacy'; But without the Additional Protocol, it may set too low a standard