BRIGHTLINE
LAWYERS

Technology | Intellectual Property | Brand

Cross-border Data Flows and Privacy Reform

Patrick Sefton | Principal, Brightline Lawyers

Cross-border data flows and Privacy Reform

- Context: IT & business process offshoring
- The current regulation and its background
  - Extra-territorial operation of Act
  - Specific regulation of cross-border data flows
- Changes to information privacy regulation
- Issues arising in the context of offshoring

Cross-border data flows – current regulation and background

Current regulation (private sector)

- NPP9 – t'fer to entity in foreign country only if:
  - Recipient legally bound similar to NPPs
  - Consent:
    - actual consent
    - disclosure for I's benefit, impractical to obtain I's consent, I would be likely to consent
  - Necessary for contract:
    - between individual and organisation
    - made in interest of individual by organisation and third party
  - Reasonable steps to ensure recipient will not use inconsistently with NPPs

Current regulation (public sector)

- IPPs – no express reference, but…
- IPP11: No disclosure (of any kind) unless:
  - Consent
  - Awareness of that kind of disclosure
  - Required by law, law enforcement
  - (Serious, imminent threat to life or health)

Extra-territorial operation

- Act can apply to overseas activities of organisations (s5B)
  - Data:
    - about Australian citizen / permanent resident (most NPPs)
    - about anyone (NPP9)
  - Organisation:
    - is Australian (eg Aus company, citizen, partnership)
    - not Australian
      carries on business in Australia
      data collected or held in Australia
  - Privacy Commissioner can investigate complaints
  - Silent on agencies

Exception: laws of other countries

- S13D(1) of the Act
  - act outside Australia not unlawful if required by an applicable law of a foreign country
  - example: compliance with other country's AML/CTF legislation, local judicial process
  - purpose: must allow organisations to comply with local law without breaching Australian law

Cases

- *E v Money Transfer Service* [2006] PrivCmrA 5
  - data sent to foreign country for money transfer to that country
  - local law triggered – name matched a watch list
  - further info requested and sent, ultimately individual cleared
  - individual complained
  - issues: NPP9, o'seas acts s5B, local law exception s13D(a)
  - Outcome s5B: collection/act in Australia therefore s13D(1) does not apply, it is the activity in Australia that is in question
  - Outcome NPP9: information given in knowledge that it would be sent o'seas to support transfer, therefore consent

Origin of the cross-border rules

- OECD Guidelines (1980)
- EU data protection directive (1995)
- Implemented in national laws
  eg *Data Protection Act 1998* (UK)
- Crisis (1998) EU considered US protection inadequate

  ("…the current patchwork of narrowly-focussed sectoral laws and voluntary self-regulation cannot at present be relied upon to provide adequate protection…")
- "Safe harbour" principles (1999): opt-in for US companies – a bridge between US & EU approaches
- Other agreements eg airline passenger lists (2002)

APEC & Data Privacy

- Australia participating (+US, +China, -India)
- ALRC cross-border proposals refer (& prefer!)
- APEC Privacy Framework (2004)
  - set of principles consistent with “core” of OECD Guidelines
  - accept that data will be universally available
  - emphasise organisational accountability for data, rather than border-controls / adequacy assessment
  - “Pathfinder” projects to facilitate accountable cross-border data flows

Acceptable contract regimes

- OECD guidance
  - Substantive rules, accountability / verification, complaint process, dispute resolution process
- EU guidance
  - published model clauses considered adequate
  - “binding corporate rules” for multinational groups
- Note Privacy Victoria also has “model terms” for cross-border data flows

Cross-border data flows – ALRC recommendations

Meaning of “transfer”

- Not as straightforward as it seems
- ALRC not willing to define
- OPC to provide examples
- May exclude information routed and stored outside Australia, but not accessed (eg email between Australian recipients)
- Will include information that is stored in Australia and accessed from overseas

Related companies

- UPP11 only triggers on transfer to a recipient (ie, different entity from the sender)
- Will not trigger if data transferred overseas by same entity (but s5B will apply)
- But will trigger if data transferred to a related company overseas

Main ALRC recommendation

- Simplify and re-cast cross-border principle on basis of:

  Adequacy, or Consent, or Accountability

  - Adequacy is the same
  - Consent provision has changed
  - Accountability is new
  - Application to agencies is new
  - Use and disclosure principle will also apply

Adequacy

- Principle same as existing regulation:

  reasonable belief that recipient subject to similar, legally-binding privacy protection

- Recognised practical difficulties
- Recommended publication of a list of "adequate" laws and schemes
- "Reasonable belief" evidenced by:
  - entry on published list
  - own legal advice

Consent

- Must be voluntary and informed
  - Individual to be advised of countries where information will be sent
  - Privacy policy to include this information
- Must be express advice of legal consequence that sender will no-longer be accountable
  - Language may be tricky here: resistance
  - Bundled consent should allow individual to consent to cross-border transfers
- OPC will issue guidance

Accountability

- “Accountable” will be defined in the Act
  - agency/organisation transfers personal information to recipient outside Australia, and
  - recipient does something that would have contravened if done in Australia, then
  - recipient's act still contravenes, and is taken to be the act of the sending agency/organisation
- That is, a vicarious liability concept for acts of overseas recipients in respect of personal information sent to them
- Only if adequacy, consent do not apply

Information Privacy Bill 2009 (Qld)

- Public consultation draft
- Information privacy for Qld agencies
  - Currently under IS42/42A
- s33 of draft relates to cross-border transfers
- More like NPP9 than UPP11
  - default prohibition rather than default accountability
  - consent, or other exceptions similar to NPP9
- Should be made consistent with UPPs.

Review of consent & disclosure, Application to offshoring

Positioning for UPP 11

- Do not want to be legally accountable to individuals for recipient's conduct
- Must ensure that one or both exceptions apply
  - Adequacy
  - Consent
- Must also amend disclosures
  - Consent
  - Privacy policy

Adequacy exception

- Jurisdiction may appear on OPCs “whitelist”
  - A complete answer
  - Likely to be slow in coming (consider EC experience)
  - Likely to be conservative, may therefore exclude important offshoring jurisdictions (India, China)
- Obtain own legal advice about jurisdiction
  - May be expensive, uncertain
- Impose by contract
  - Substantive rules based on UPPs (at minimum)
  - Should have verification, dispute resolution provisions
  - Local-law advice, jurisdiction provision

Existing offshoring contracts

- May need to be reviewed to confirm that they still subject recipient to regime substantially similar to (new, UPP) principles
- Depends on existing drafting, how liberal are existing arrangements

Consent exception

- Two issues
  - “Informed consent” means advising where the data may be going overseas (and to what countries)
  - UPP11 exception calls for express disclosure that consent will remove sender's accountability for the data
- Will need to review & consider existing consents and forms of consent
  - whether the data will go overseas?
  - which countries?
  - insert additional disclosure about accountability (this will need to be fairly blunt)

Example consent

You consent to the disclosure of personal information about you to our service providers for the purpose of processing that information on our behalf.

You understand that such providers may be located in other countries including [India] and [China], and the information may be transferred to providers in those countries for processing.

You understand that giving this consent means that, although providers will be subject to strict confidentiality and security controls, we will not be "accountable" (within the meaning given in the Privacy Act) for the information, once transferred.

Privacy Policy

- Will need to be reviewed to include
  - whether personal information may be transferred outside Australia
  - the countries to which such information is likely to be transferred
- That information was not, historically, thought necessary in a privacy policy, and was not usually included

Related companies and “captives”

- UPP 11 will apply to transfers to related companies overseas
- Less concern about accountability
  - But note captive will not necessarily always be so
  - Advisable to obtain consent,
    confirm adequacy by intra-group contract

Removal of exceptions

- Employee records exemptions removed
- Offshored payroll processing would be covered (note that payroll is the second most popular outsourcing target, after IT)
  - communication to to employees
  - will consent be sought, or rely on adequacy
- Small business will also be covered for the first time

BRIGHTLINE LAWYERS

Technology | Intellectual Property | Brand

Thank you.

Patrick Sefton
patrick.sefton@brightline.com.au