BNA International

World Data Protection Report

International Information for International Businesses

Monthly news and analysis of data protection and privacy issues from around the world

Volume 9, Number 1 January 2009

Commentary

News

News

BNA International Inc., a subsidiary of The Bureau of National Affairs, Inc., U.S.A.

The Australian *Dodo* Case: an insight for data protection regulation

By Malcolm Crompton, Managing Director, Christine Cowper, Principal Consultant and Christopher Jefferis, Research Consultant, at Information Integrity Solutions (IIS). They can be contacted at: MCrompton@iispartners.com, ccowper@iispartners.com and cjefferis@iispartners.com*

Introduction

In a global economy the way in which cross-border data flows are regulated can significantly affect the efficacy of national privacy or data-protection regimes and ultimately the confidence of individuals in transactions or activities based on those data flows. An approach based on clear and full 'accountability' of all the parties involved in such data transfers, especially the transferor, is emerging as a preferred alternative to relying on an assessment of the 'adequacy' of data protection regime in other countries to protect consumers.

The concept of accountability addresses a complex issue in a way which, importantly, is simple, pragmatic and potentially more 'future proof' than other approaches; for example it is simpler for consumers to make a complaint and it also facilitates investigation and enforcement by the regulator. A growing body of evidence from regulators who cover personal information in a number of countries and also from regulators in other spheres suggests that the accountability approach can significantly improve governance of business practices which are conducted across international borders. Indeed, the Australian Law Reform Commission recommended an approach based on accountability in its extremely thorough review of Australian privacy law, "For Your Information: Australian Privacy Law and Practice" in 2008.[1]

A recent Australian case under the *Do Not Call Register Act 2006* (DNCR Act) which regulates telemarketing calls to households, provides a demonstration of how an accountability approach could work in practice. Important elements in the story also include the construct of the law and the strategic approach taken by the regulator. It is the so-called *Dodo* Case.

The Accountability and Adequacy models explained

The objective of protecting personal information when it moves between jurisdictions is becoming rapidly more important. It is already being addressed in multi-lateral forums such as the Asia-Pacific Economic Cooperation forum (APEC)[2] and the Organisation for Economic Co-operation and Development (OECD)[3]. One way in which the objective can be understood is in terms of eliminating the additional 'country risk' imposed on individuals when an organisation or government agency sends personal information about them to another country. Around the world, two approaches have emerged as most often applied to achieving the objective of reducing or eliminating this 'country risk' for the individual.

One approach is based on the concept of 'adequacy'. The 'adequacy' approach seeks to ensure that the receiving country or jurisdiction is perceived as having an 'adequate' privacy protection law in place. Most notably, this approach has been taken by Directive 95/46/EC of the European Parliament dated October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (E.U. Directive).

The other approach is based on the concept of 'accountability'. This approach ensures that the original collector of the personal information remains accountable for compliance with the original privacy framework that applied when and where the data was collected, regardless of the other organisations or countries to which the personal data travels subsequently. It is already included in the privacy frameworks of some privacy jurisdictions including Canada and the United States of America as well as the APEC Privacy Framework.[4]

The effectiveness of either an 'accountability' or 'adequacy' based regime will in part depend on the legal powers and financial resources available to those who carry the responsibility for enforcement including the regulators. However, the accountability approach has a particularly good chance of working effectively because of the construct that it is the responsibility of the trans-

feror to ensure that appropriate information handling practices are safe in the first place and remain safe.

The following brief observations point to some of the practical consequences of the two theoretical models and, in the authors' view, brings the strengths of the accountability approach into focus.

The concept of adequacy implies the need to make assessments of the data protection regimes in countries to which personal information may be transferred. In the E.U. context adequacy is determined by the Article 29 Working Party of data protection regulators who assess the conditions of data transfer, the rule of law and security measures in place in that country. As an observer of the process it can be difficult to see consistency in the basis on which the 'adequacy' decisions are made. There is a mixed list of jurisdictions and programs which have achieved adequacy including: Canada, Switzerland, Argentina, Guernsey and the Isle of Man, Jersey, the U.S. Department of Commerce's Safe Harbor Privacy Principles and the 'transfer of Air Passenger Name Records to the United States Bureau of Customs and Border Protection'.[5] Other jurisdictions with privacy law and demonstrably more effective rule of law have not been found adequate, including Australia.

Arguably the adequacy approach is also hard for the consumer and regulator to work with. Importantly, the approach does not provide consumers with a coordinated way of making and handling a complaint should a breach occur in another country. It has also led to little impetus for cooperative arrangements between regulators, something that is arguably more important in an adequacy model than an accountability model.[6] All that is needed is a finding that the law in the other jurisdiction is by itself 'adequate'.

In effect, the adequacy model places the responsibility on the consumer to make preliminary investigations, before they can make a formal complaint. For example they would need to find the relevant regulator or accountability body in relevant jurisdictions where the alleged breach might have occurred. If somebody feels something has gone wrong with their personal information and it looks like it involves activity in multiple jurisdictions, then it is normally the complainant who has to work out which jurisdictions might be involved and to which jurisdiction they should take the complaint. There is often nobody in officialdom who will help them do this – they are on their own, although advocacy bodies such as the Australian Privacy Foundation or in the United States the Electronic Privacy Information Center may be of considerable help. But with today's technologies this can be a seriously difficult forensic task requiring resources and capability beyond most individuals.

At least some if not all of the above also apply to any regulators that have direct jurisdiction, or are willing to assist a citizen, to pursue a complaint against organisations in other countries. They too would have to work out which jurisdictions are involved, get in touch with colleague regulators who may or may not want to cooperate and/or pursue in other courts. Moreover, the actual supporting powers forcing/allowing/preventing cooperation vary hugely between regulators. The SAFE WEB Act in the United States gives the Federal Trade Commission quite good but still limited powers to cooperate with regulators overseas yet it appears to have placed the FTC in a better position than most other privacy regulators. Indeed, some other regulators face legal barriers to cooperation. The Privacy Commissioner for Personal Data, Hong Kong, for example, appears to be prevented in law from sharing a case file with another regulator even if the complainant consents or asks for it.

Moreover, even if the individual can identify the relevant regulator they may not have standing to pursue the complaint. For example, until the Australian *Privacy Act 1988* was amended in 2004, individuals who were neither Australians nor resident there had no standing to seek to have inaccurate personal information corrected or to seek redress for mishandling of personal information transferred to another country.[7]

By contrast, the accountability approach is less reliant on the arrangements in the country to which data has been transferred. In many cases under the accountability approach, for example the *Dodo* case discussed below, all the regulator has to do is enforce the law on the 'first in the chain' in regard to the full misdeeds of anybody in the chain including those further along. What that first entity in the chain does about it after paying the fines and providing full restitution is up to it (be it sharing the penalties *etc* by enforcing contracts or absorbing the total costs). If the problem continues, the first in the chain keeps on paying up and otherwise providing restitution. For the regulator and the complainant, the job is done.

Importantly, this means that a lot of the enforcement action is not being done by either the affected individual or the regulator. It is outsourced to the initial party to the misdeed; a rather nice application of the Mikado principle of letting the punishment fit the crime.

The *Dodo* Case

The *Dodo* case provides an example of how readily the accountability approach can be applied and again shows the potential strengths of the model. In the *Dodo* case, the responsible regulator, the Australian Communications and Media Authority (ACMA) fined an Australian based telecommunications provider, Dodo Australia Pty Ltd (Dodo), $147,000 because of persistent telephone marketing to individuals who had subscribed to the Australian Do Not Call register.

As ACMA points out in its commentary on the case, even if a business decides to use offshore call centres to make calls, it will be responsible for the calls that those call centres make.[8]

The DNCR Act provisions and enforcement mechanisms

In Australia the DNCR Act was introduced in response to increasing community concern about unsolicited

  WDPR ISSN 1473-3579

telemarketing calls. The Act allows individuals to opt out of receiving a wide range of unsolicited telemarketing calls by listing their telephone number on a register. From May 31, 2007 it became illegal, in the absence of consent or other specified conditions, for any non-exempt telemarketer in Australia, including off-shore telemarketers contracted by Australian businesses, to contact a number listed in the register.[9] Telemarketers are able to 'wash' their lists against the register to ensure they do not make calls that would breach the DNCR Act.

ACMA as the relevant regulator is responsible for overseeing the operation of the do not call scheme, the register and for investigating breaches of the DNCR Act. It also has the power to set additional industry standards, which it has done for example in relation to the permitted times to make telemarketing or research calls to domestic residences. The enforcement model for the Act relies to some extent on individuals making complaints about unsolicited telemarketing calls, to the organisation, the register operator, or to ACMA. However, it also provides ACMA with a considerable range of powers to investigate and deal with significant or potentially systemic matters.

The Act then provides a tiered enforcement regime based on a range of enforcement measures that can be initiated by the ACMA, depending upon the seriousness of the breach, consistent with the principles of good Responsive Regulation.[10] The enforcement measures available to the ACMA include a formal warning, acceptance of an enforceable undertaking, or the issuing of an infringement notice. The ACMA may also apply to the courts for an injunction or to institute proceedings for breach of a civil penalty provision. As well as ordering a person to pay a substantial monetary penalty, the Court may make an order to recover financial benefits that are attributable to the contravention of the civil penalty provision, or may order compensation to be paid to a victim who has suffered loss or damage as a result of the contravention[11] .

The DNCR Act also contains two key provisions which are particularly relevant when considering the regulation of cross border data transfers. They are:

- S.11(1) which provides that an organisation must not make or cause a telemarketing call to a registered number; and

- S.12 which provides that agreements regarding telemarketing calls must require compliance with the DNCR Act.

S.11(1) was designed to ensure that the DNCR legislation covered calls made from overseas to Australian numbers on the register[12] . This provision allows ACMA to hold Australian organisations responsible under the Act for the activities of overseas telemarketers with whom they contract.

ACMA's *Dodo* investigation

ACMA commenced its formal investigation after receiving over 100 complaints from individuals who stated that they received telemarketing calls from Dodo at a time when the numbers called had been listed on the register for more than the required 30 days. It initially sent Dodo an advisory letter in June 2007 which was followed up with a warning letter in July 2007 that provided examples alleging that an off-shore call centre had made calls to numbers on the register on its behalf. ACMA commenced investigations into Dodo's off-shoring activities in October 2007. It found that one of the three call centres Dodo had contracted did call registered numbers. Dodo claimed that it had taken reasonable precautions to ensure that its contractors had complied with the DNCR Act. However, ACMA found that Dodo had not exercised due diligence and that Dodo had contravened the Act.[13]

ACMA concluded its investigation of Dodo in July 2008. It accepted enforceable undertakings from Dodo aimed at ensuring future compliance. ACMA also issued an infringement notice to Dodo Australia for 67 alleged contraventions of the DNCR Act. The sum which Dodo was required to pay under the infringement notice of $147,000 is the largest penalty paid since the DNCR Act came into effect in May 2007.

The penalties for breaching the DNCR Act 2006 could have been higher if the matter had proceeded to court but Dodo cooperated with ACMA's investigations and eventually responded proactively to the issues.

The *Dodo* case – an accountability model exemplar

Development of the Internet and telecommunications technology has created a global marketplace for services such as telemarketing and processing of personal data. In particular, many businesses have opted to take advantage of the cost reductions that the global marketplace can provide by off-shoring these types of business activities to overseas service providers. There are likely to be advantages to businesses and consumers but there are also clear risks; in the *Dodo* case they included unexpected and unwelcome telemarketing calls.

The question here is not whether businesses should outsource offshore but rather how can a government and regulators protect their citizens where businesses are conducting their operations outside of their jurisdiction.

The *Dodo* case provides a useful illustration of helpful elements in the design of a data protection regime; some of these elements are particular to the accountability approach and show the potential strengths of that model. The key points worth noting are as follows:

- The legislative framework, the DNCR Act, is cleverly designed; as noted earlier it specifies the activities it is seeking to control both in terms of *making* telemarketing calls and *causing* telemarketing calls to be made. This provision was specifically included in recognition

of the possibility of outsourcing including to overseas-based organisations and set up the conditions to enable the accountability principle of holding the 'first in the chain' responsible. Moreover the DNCR Act provides a simple central mechanism for a consumer to raise concerns. The scheme provides for issues to be considered by the register operator and to be escalated to ACMA where matters cannot be resolved. In practice, consumers got action in response to a relatively simple complaint to the local regulator.

- In addition, the DNCR Act, together with the *Telecommunications Act 1998*, gives ACMA a wide and flexible range of functions and powers to draw upon, providing a framework consistent with good Responsive Regulation principles and means that ACMA is able to escalate its action until it can get a result and to apply a regulatory response proportional to the nature and extent of non-compliance.

- ACMA used its powers with strategic intent (something that Responsive Regulation framework enables but that still has to be deployed): ACMA knew what it was doing, for example, in terms of identifying where to target its effort to gain the greatest effect, had a plan, and carried it out. This is consistent with the 'three Es framework' that any regulator needs to apply, that is action that is ethical, effective and efficient.[14]

  In this instance, ACMA chose to hold Dodo, which 'caused' the calls to be made, accountable for compliance with the DNCR Act rather than the organisations which actually made the calls, in this case from India. Instead of investigating the Indian call centres which would have been more resource intensive because there were more organisations to consider and they could be hard to contact and hold accountable, it focused its powers and enforcement action on the point of the chain where it had the most leverage – the organisation in Australia which initially cause the calls to be made. Indeed, anecdotal evidence indicates it was even more effective than ACMA had anticipated.

- ACMA was able to apply leverage, that is to take action against one party, Dodo, and have direct impact on all parties to whom Dodo contracted and indirect impact on the whole market. It had direct bottom line impact on call centre finances through lost opportunities to sell services to Australian business which focused the mind more than any direct attempt at prosecution. This is more a characteristic of accountability than adequacy.

- ACMA was able to apply the leverage efficiently (and effectively) by taking the action against an organisation that operated directly within its home jurisdiction, a key characteristic of accountability but not adequacy.

- Neither ACMA nor any other regulator had to worry about enforcing anything in India – that was up to Dodo, either by taking action against its off-shored service providers for past misdeeds and/or ensuring that future service providers were compliant, a key characteristic of the accountability approach that is not characteristic of the adequacy approach.

Conclusion

Global business operations, which are conducted across international borders and involve cross-border data flows, pose significant governance challenges. The inherent characteristics of accountability, which start from the notion that it is the responsibility of the transferor to ensure that appropriate information handling practices are safe in the first place and remain safe, appear to make it the approach of choice over adequacy. This is borne out by a recent Australian case, the *Dodo* case; Dodo as the organisation responsible for initiating the activity ultimately bore the penalty for the 'unsafe' practices of its contracted overseas partner.

That said, whether any regulatory framework will be effective depends on a number of characteristics including the legal, financial and moral mandates of the regulator and its strategic capability.

** IIS is a specialist privacy consultancy; its services include privacy impact assessments, privacy thought leadership and advice and strategy. Information about IIS is available at http://www.iispartners.com*

NOTES

[1] Available online at http://www.alrc.gov.au/media/2008/mr11108.html; Chapter 31 deals with trans-border data flows and is online at http://www.austlii.edu.au/au/other/alrc/publications/reports/108/31.html

[2] As epitomised by the focus of the APEC Data Privacy Subgroup since 2007 on a Pathfinder initiative to address the protection of personal information when it moves between economies; see for example the description at http://www.dpmc.gov.au/privacy/apec/pathfinder_initiative.cfm; for details of the component projects in the Pathfinder, see "APEC Data Privacy Pathfinder Projects Implementation Work Plan", document No 2008/SOM1/ECSG/024 submitted to the 17th Electronic Commerce Steering Group Meeting, Peru, February 24, 2008 at http://aimp.apec.org/Documents/2008/ECSG/ECSG1/08_ecsg1_024.doc

[3] See http://www.oecd.org/sti/privacycooperation for a summary of the OECD work.

[4] For example, the APEC Principle 9 states that accountability remains with the original personal information controller, even if the information is passed on to others unless the transfer occurs with the individual's consent. The Department of the Prime Minister and Cabinet of Australia provides a succinct, collated source of information about the APEC privacy framework at http://www.dpmc.gov.au/privacy/apec/apec_privacy_framework.cfm. See also the web page for the APEC Electronic Commerce Steering Group, to which the APEC Data Privacy Subgroup reports, and a full copy of the framework, at http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html

[5] See "Commission decisions on the adequacy of the protection of personal data in third countries", on the European Commission website as at January 3, 2009, http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_en.htm

[6] Yet it is in the APEC context where the cross-border privacy framework is built on the accountability model that the most progress is being made on developing such cooperative arrangements, as detailed in earlier footnotes.

[7] See the E.U. submission to the Australian Parliament identifying the problem at http://www.aph.gov.au/House/committee/laca/Privacybill/sub113.pdf. The Parliament addressed the problem in the Privacy Amendment Act 2004, at http://www.comlaw.gov.au/

  WDPR ISSN 1473-3579

ComLaw/Legislation/Act1.nsf/framelodgmentattachments/3C45936C4195887ACA25744700026DEE

[8] See ACMA's media release announcing the conclusion of its investigation available at http://www.acma.gov.au/WEB/STANDARD/pc=PC_311469

[9] For detailed information about the DNCR Act and scheme see http://www.acma.gov.au/WEB/STANDARD/pc=PC_100642

[10] See "Responsive Regulation – Transcending the Deregulation Debate" by Ian Ayres and John Braithwaite, 1992, http://www.oup.com/us/catalog/general/subject/Politics/AmericanPolitics/?view=usa&ci=9780195093766, presented by John Braithwaite to the First APEC Technical Assistance Seminar on Cross-Border Privacy Rules in January 2007, http://aimp.apec.org/Documents/2007/ECSG/SEM1/07_ecsg_sem1_019.pdf and summarised in a Seminar Background Paper for participants in the Second Seminar that year http://aimp.apec.org/Documents/2007/ECSG/SEM2/07_ecsg_sem2_002.doc

[11] Do Not Call Register Act 2006 Explanatory Memorandum p 2. See http://www.austlii.edu.au/au/legis/cth/bill_em/dncrb2006211/memo_0.html

[12] Ibid; pp 58-59.

[13] For details of ACMA's findings and the results of the investigation see the enforceable undertaking given by Dodo to ACMA available at http://www.acma.gov.au/webwr/_assets/main/lib310480/dodo_aust_pl_s572b_enforceable_undertaking.pdf

[14] The distinction between what is required in regulation and what is required of the regulator within that regulatory framework is too rarely made. For an earlier account of these issues including the development of the three Es concept see "Light Touch or Soft Touch – Reflections of a Regulator Implementing a New Privacy Regime", first delivered by Malcolm Crompton as Privacy Commissioner to the National Institute of Governance at University of Canberra, in March 2004, http://www.privacy.gov.au/news/speeches/sp2_04p.pdf.