International Journal of Law and Information Technology Vol. 17 No. 2 © Oxford University Press 2007; all rights reserved
doi:10.1093/ijlit/eam004 Advance Access Published on 13 August 2007

The "Final" Privacy Frontier? Regulating Trans-Border Data Flows

Gehan Gunasekara*

Abstract

This article examines the threat to privacy posed by the transfer of personal information from one jurisdiction to another. Despite international trends towards greater protection of personal information significant challenges to personal privacy arise in this context. These include the use of outsourcing by businesses, the encroachment of security laws and the potential 'spill-over' of technologies developed for combating terrorism into the private sector. Also significant are technologies enabling the 'profiling' of individuals and 'data mining' across borders. Against this backdrop the article considers existing jurisdictional responses towards regulating personal information flows across borders. It considers various actual or proposed solutions including 'safe-harbours', contractual mechanisms and extra-territorial applications. The article concludes that many of the existing approaches to regulating trans-border information flows are to some extent deficient and suggests the need for a new 'fourth generation' set of data protection protocols. In formulating the latter, analogies are drawn from other relevant areas of the law in order to furnish creative solutions to the problem.

* Senior Lecturer in Commercial Law, University of Auckland. I am grateful to Alexandra Sims for her helpful comments on an earlier draft of this article. All errors are, of course, my own. g.gunasekara@auckland.ac.nz

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

1 Introduction: Some Practical Illustrations

The blood running through the veins of twenty-first century commerce will increasingly consist of information about individuals. The needs of individuals are progressively better able to be catered for because technology can, as never before, track and predict their behaviour. However the ever-increasing technological capabilities of businesses and governments, to collect compare and transmit personal data, combined with the increasingly paranoid attitudes of many governments in tackling security concerns, presage an Orwellian surveillance society on a global scale. This article assesses the risks involved in the flow of personal data between jurisdictions and evaluates the adequacy of existing regimes in response to it.

I preface the discussion that follows with three scenarios, all of them actual or current controversies, in order to illustrate the nature of the subject matter involved.

First, a New Zealand resident of South Asian descent (with a common South Asian name) wishes to urgently transfer a sum of money to India in order for his uncle to obtain a kidney transplant operation. He engages the services of Western Union, an American money-transfer company, through their New Zealand agents, NZ Post. The money is never received in India and instead is frozen for nearly a month before it is handed back to the individual concerned. Only after the money was frozen did Western Union advise the individual that his name had been checked against international terrorist lists.[1] The company ultimately sends the individual a letter of apology.[2]

Second, the Government of the Canadian province of British Columbia proposes to contract out the administration of its public health insurance program, the Medical Services plan, to a Canadian subsidiary of an American company. Critics argue that this could result in United States agencies including the Federal Bureau of Investigation (FBI) obtaining personal information about Canadians from American companies as a result of the operation of the provisions of the United States PATRIOT Act.[3] The ensuing controversy results in litigation,[4] amending Canadian legislation[5] and a comprehensive investigation by the British Columbia Office of the Information and Privacy Commissioner.[6]

---

[1] Several watch lists exist including, in the United States, that of the Office of Foreign Assets Control (available at: http://www.treasury.gov/offices/enforcement/ofac/sdn/t11sdn.pdf) as well as a United Nations list.

[2] For an account of this incident see the *Weekend Herald*, Saturday-Sunday, October 23-24 2004, A16.

[3] This is discussed further below.

[4] *British Columbia Government & Service Employees' Union (petitioner) v The Minister of Health Services and The Medical Services Commission (respondents)* B.C.S.C., Victoria registry No. 04-0879.

[5] Freedom of Information and Protection of Privacy Amendment Act, 2004, S.B.C. 2004, c.64.

[6] Information & Privacy Commissioner for British Columbia 'Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing', (British Columbia, 2004). Available at: http://www.oipcbc.org/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

The final example concerns the electronic transfer, by airlines flying to and from the United States, of so-called 'Passenger Name Record' (PNR) data[7] to the United States Department of Homeland Security Bureau of Customs and Border Protection (CBP). Following the terror attacks of September 11, 2001, this requirement has been imposed by the US authorities. However the requirement on airlines to hand over information collected for one purpose (providing a service) for another purpose (data-mining for security-related purposes and for combating terrorism) contravened the strict privacy rules contained in European Union legislation (hereafter the 'Privacy Directive')[8] thereby placing the airlines in something of a dilemma. In May, 2004 the European Commission ruled that privacy undertakings given by the CBP were 'adequate' thus allowing for the transfer of the data. However this decision was challenged and on May 30, 2006 the European Court of Justice ruled that the transfer of PNR data to CBP constitutes processing operations concerning public security and the activities of the State in areas of the criminal law, matters outside the ambit of the Privacy Directive in the first place. The Commission was therefore not empowered to grant an 'adequacy' exemption from the requirements of the Privacy Directive.[9] At the time of writing this impasse has yet to be resolved.

There are common threads running through the foregoing illustrations. An obvious one is that they all relate to security and counter-terrorist measures but this is purely co-incidental. To be sure, the encroachment of security imperatives into areas traditionally regarded as private and personal to individuals represents a challenge for privacy values and is one focus for discussion in this article.

The real lesson contained in the examples, however, is more mundane. It is that in an increasingly globalized world, where the market for goods and services spans national borders, national safeguards and regimes for the protection of personal data or information about individuals is of little value as technology allows the information to be whisked out of the jurisdiction at the proverbial click of a mouse. The discussion below examines the challenge posed by these developments against the various jurisdictional responses to them. It will be seen that, despite significant convergence in global information privacy norms, the difficulties resulting from trans-border data flows represents a further concern insufficiently dealt with by existing privacy norms. This may necessitate a new,

[7] The PNR data elements include the 'PNR record locator code,' date of reservation, name, address, all forms of payment information, contact telephone numbers, travel agency, travel status of the passenger, e-mail address, general remarks, seat number, no-show history and any collected APIS (Advanced Passenger Information System) Information.

[8] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data; this directive is discussed further below.

[9] *European Parliament v Council of the European Union*, ECJ, C-317/04 & C-318/04, 30 May 2006.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

Fourth Generation, of Data Protection Principles. If so the result would be ironic as the original impetus for uniform data protection standards was to alleviate concerns by business and governments that differences among national laws might hamper the free flow of personal data across borders and hinder economic development.[10] Acceptance that a new set of criteria are needed would represent an acknowledgement of at least a partial failure of this objective. Whether a new set of principles, addressing the flow of personal information across borders, will amount to the 'final' step, in creating a global privacy framework, only time will tell. However some solutions are tentatively suggested in this article.

2 The Evolution of Global Information Privacy Norms

The recognition of privacy as a concept worthy of distinct treatment by law is a relatively recent development and dates back to a seminal article by two Harvard academics at the end of the nineteenth century.[11] The likely impulse for this essay was the perceived danger of the technology of the day, cameras and mass-circulation newspapers. The twentieth century saw the extensive development of several distinct torts of privacy in the United States[12] and the tort has continued to be modified and adopted in different ways in other common law jurisdictions including the United Kingdom[13] and New Zealand.[14]

In more recent times fresh privacy concerns again arose as a result of technological developments, notably the spectacular growth of automatic data processing made possible by the computer revolution. While their use was at first limited to large government agencies for purposes such as policing, taxation and social security[15] large private sector firms rapidly followed suit and the continued evolution of computers, telecommunications networks and eventually the internet meant that unprecedented amounts of information about individuals (personal data or personal information) could be collected, stored and transmitted by even the smallest of private-sector firms with relative ease. In addition, the ability to 'profile' individuals' behaviour, purchasing patterns and creditworthiness led

[10] See for example the OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data,* 1980, clause 17.

[11] SD Warren and LD Brandeis 'The Right to Privacy' (1890) 4 *Harv LR* 193.

[12] *Restatement of the Law of Torts, 2d* (American Law institute: 1965-79) S 652A-F.

[13] Through application of the existing remedy of Breach of Confidence although influenced heavily by the Human Rights Act 1998 (UK) which implemented the European Convention on Human Rights see *Campbell v MGN Ltd* [2004] 2 AC 457 (HL).

[14] *Hosking v Runting* [2005] 1 NZLR 1 (CA).

[15] Early concern in New Zealand over privacy led to the enactment of the Wanganui Computer Centre Act 1976 which for the first time contained provisions safeguarding personal privacy of citizens.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

to fears as to the arrival, by stealth, of the ultimate surveillance society. Big Brother may not necessarily be the State or Government apparatus but may indeed exist all the same in terms of an individual's ability to control what information is known about them and by whom.

The counterpart to data matching by government agencies (for example between taxation authorities and social welfare or immigration) is the very real possibility of the exchange or sale of data between companies. For instance a health insurance provider may find a potential customer's dietary preferences (easily obtainable from supermarkets through the use of loyalty cards and the like) of value in order to 'customize' the level of risk and premium to that customer. In an age of consumer credit the 'credit-worthiness' of individuals and their consumer preferences are also obvious targets for business to exploit. Commentators have long ago observed that we live in an information age and that personal information clearly is of value.[16] The economic importance of an increasingly affluent global middle class was evident. The issue, however, was the type of regime which should govern the collection and disposal of information about these individuals.

The response to these trends originated in the more advanced economies of the West. From the early 1970s onwards countries such as Sweden, France and Germany enacted legislation which applied to both the public and private sectors. One of the earliest privacy statutes was the United States Privacy Act of 1974[17] which remains in force. This statute only applies to personal information about citizens held by the federal government however. To harmonise standards and prevent the free flow of information between the advanced economies the Organisation for Economic Cooperation and Development (OECD) developed, in 1980, a set of principles known as the Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data.[18]

The legislation and the OECD Guidelines contained common elements. The 'rules' they set out were open-ended and structured in the form of guidelines or principles. Ultimately they came to be known as 'fair information practices' or 'data/privacy protection principles.' The principles themselves are astonishingly uniform. A typical example is the ten privacy principles contained in Canada's federal privacy law, the Personal Information Protection and Electronic Documents Act (PIPEDA).[19] These have been summarised as:

1. *Accountability.* Organizations are accountable for the protection of personal information under their control.

[16] See for example Anne Wells Branscomb, *Who Owns Information? From privacy to public access* (Basic Books, New York, 1994).

[17] 5 USC S 552(a) (1988).

[18] Available at: www.oecd.org.

[19] Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

2. *Identifying purposes.* The purposes for which the personal information is being collected must be identified during or prior to the collection.

3. *Consent.* Information must be collected with the knowledge and consent of the individual and for a reasonable purpose.

4. *Limiting collection.* The collection of personal information is to be limited to what is necessary for the identified purposes and must be collected by fair and lawful means.

5. *Limiting use, disclosure and retention.* Information can only be used and disclosed for the purpose for which it is collected and be retained only as long as it is necessary to fulfil the purpose.

6. *Accuracy.* Information must be as accurate, complete and up-to-date as possible.

7. *Safeguards.* Information must be protected by adequate safeguards.

8. *Openness.* Information about an organization's privacy policies and practice is to be readily available.

9. *Individual access.* Information must be accessible for review and correction by the individual whose personal information it is.

10. *Challenging compliance.* Organizations are to provide means to an individual to challenge an organization's compliance with the above principles. [20]

Jennifer Stoddart, the Privacy Commissioner of Canada has succinctly explained the effect of the principles:

> People should be told what information is being collected about them, by whom, for what purposes; they should be told what is being done with it and who it is being disclosed to; they should be able to control the collection, use and disclosure of the information through the power of granting or withholding consent; the information should be securely held and treated as confidential; people should have a right of access to their information, and a right to correct it where necessary. [21]

Similar principles are contained in the privacy legislation of several other jurisdictions, for example the twelve Information Privacy Principles in New Zealand[22] and the ten National Privacy Principles in Australia.[23]

---

[20] Above n 6, at p 38.

[21] Privacy Commissioner of Canada, 'Annual Report to Parliament 2003-2004' (available at: http://www.privcom.gc.ca/information/ar/200304/200304_e.asp).

[22] Privacy Act, 1993, s 6.

[23] Privacy Amendment (Private Sector) Act 2000 (C'th, Aust).

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

The Privacy Directive of the European Union was itself the impetus for many of these, including the Australian enactments. The laws pertaining to information privacy therefore share common characteristics. To use a biological metaphor; they possess the same DNA. If one were to extend the metaphor further, however, the most advanced evolutionary form of data privacy regime is that of the European Union.

Although a consensus may exist as to the content of the information privacy principles themselves the same cannot be said about their implementation. A majority of jurisdictions have followed the European approach in creating a 'seamless' web of protection spanning both private and government spheres, thus recognising that information can easily be transmitted between sectors and the reality that private/public distinctions are virtually impossible to maintain in an age of outsourcing and contracting out of public services. New Zealand,[24] Australia[25] and Hong Kong[26] have also followed this approach as, most recently, has Japan.[27]

In the United States, on the other hand, information privacy law has developed differently. Despite privacy rules being adopted at an early stage for the Federal Government similar provisions have not been developed spanning the private sector. Instead a number of ad-hoc measures have been enacted, often in response to egregious violations,[28] sector by sector. These include the Family Education Rights and Privacy Act 1974 (relating to student records), the Right to Financial Privacy Act 1978 (relating to bank records), the Fair Credit Reporting Act 1970 (relating to credit reporting), the Children's Online Privacy Protection Act (COPPA) 1998, the Health Insurance Portability and Accountability Act 1996 and the Driver's Privacy Protection Act 1994. This patchwork scheme of protection is well short of the degree of privacy protections existing in jurisdictions that have followed the European approach, an approach which due to its seamless nature minimises the opportunities for information to fall into the gaps between diverse regulatory provisions. Privacy experts generally agree that in the United States, the gathering, sharing, selling and use of personal and consumer information is largely unregulated outside the health care and banking sectors.[29]

In addition, a major weakness in the United States approach is the absence of a federal Data Protection Office or Commissioner to investigate complaints by individuals and to promote information privacy values.

[24] Privacy Act 1993.

[25] Privacy Act 1988 (as amended) (C'th, Aust).

[26] Personal Data (Privacy) Ordinance 1996.

[27] Personal Information Protection Act (Law No. 57 of 2003).

[28] For example the Video Privacy Protection Act 1988 was enacted by Congress as a result of the release of Judge Robert Bork's video rental records during his failed Supreme Court nomination.

[29] Above n 6, at p 51.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

Most other jurisdictions have a Privacy Commissioner. In countries with 'third generation' privacy laws, such as New Zealand, all forms of personal information are protected, regardless of the media in which they are contained and, fundamentally, the same rules apply to all agencies that collect and process personal information, whether they be large governmental organisations or private business entities such as pizza delivery franchises or mail order firms.

A caveat must be added to any discussion concerning information privacy. Privacy can theoretically be categorised into various branches, for example physical privacy, territorial privacy and information privacy. It is only the last of these, information privacy, which is the subject for discussion in this article. However for practical purposes the categories do overlap. For instance if one considers the present day phenomenon of so-called 'extraordinary rendition' of terrorism suspects by the United States[30] it becomes apparent that information gathered about individuals may well result in extremely adverse consequences to those individuals in physical terms. Hence it becomes all the more important to know what personal information is being gathered, by whom and for what purpose. As a consequence the arguments advanced by some commentators that information privacy, or even privacy itself, ought to be accorded a lower status to that of other legal rights such as the right to liberty are, with respect, fundamentally flawed.[31]

3 The Cross-border Challenge

The divergences between the United States and other jurisdictions that have made provision for the protection of personal data represented a serious and urgent challenge to the goal of achieving uniform global standards for information privacy. The case for reconciling the different approaches was particularly cogent given the substantial volume of world trade in goods and services that flowed between the United States and the European Union. However differences between these giant economic blocs were not the only challenge faced by advocates of information privacy protection. Some of these other challenges are briefly mentioned below.

3.1 *The Business Challenge: Outsourcing*

The transfer of personal information across borders was a troubling enough issue when privacy norms differed between the jurisdiction

[30] Involving the alleged extra-legal abduction and transfer of suspects to 'black-sites' in third countries where they have been allegedly subject to detention, torture and interrogation; see P Sands 'The International Rule of Law: Extraordinary Rendition, Complicity and its Consequences' [2006] *European Human Rights LR* 408.

[31] See for instance C Doyle and M Bagaric, *Privacy Law in Australia* (The Federation Press: Sydney 2005) at pp 50-56.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

from which the information was sent and that in which it is received. Of far greater concern, however, is the fact that, increasingly, personal information is being sent to jurisdictions where little or no protection exists for the data. Technological advances and trade liberalisation have enabled the flow of personal information in the course of data management services to countries like India and China.[32] These trends are likely to see not only personal information flows to English-speaking parts of the Third World but in all probability, to francophone Africa and Latin America as well. Indeed, the outsourcing of 'knowledge work' has been described as the third wave of globalization, following trade and manufacturing.[33]

There is no reason to automatically fear these developments. On the contrary, they may provide a spur for developing countries to bring their information privacy laws into line with those of developed nations. For example, Argentina enacted legislation and became the first Latin American country to obtain an adequacy ruling from the European Commission.[34] India is in the process of enacting a comprehensive data protection law.[35]

Nevertheless, concern over the privacy implications of outsourcing has led to members of the European Parliament (at the instigation of labour unions) seeking an inquiry by the European Commission as to whether data protection rules were breached in the outsourcing of British businesses' functions.[36] In the United States concerns over outsourcing led to the introduction in the House of Representatives of a law designed to ensure that data protection laws in offshore jurisdictions meet stringent standards.[37] The Privacy Commissioner for British Columbia has referred to the irony of the latter proposal given European concerns, discussed below, that American privacy rules themselves are inadequate.[38]

The implications of outsourcing for privacy have been examined by the British Columbia Privacy Commissioner in a meticulously researched report.[39] The conclusion was that a ban on outsourcing was neither practicable nor desirable but that safeguards were nonetheless required.[40] Some of the suggested solutions will be explored further in this article.

---

[32] Above n 6, at p 44.

[33] Public Policy Forum and ITAC Round Table, 'IT Offshore Outsourcing Practices in Canada' (Ottawa, 20 May 2004) at p 6.

[34] The process of satisfying the European Commission under the Privacy Directive is explained below.

[35] See generally the discussion in Dorothee Heisenberg, *Negotiating Privacy: The European Union, the United States, and Personal Data Protection* (Lynne Rienner Publishers, USA, 2005) at pp 112-113.

[36] Ibid.

[37] US, Bill H.R. 4366, Personal Data Offshoring Protection Act of 2004, 108th Cong., 2004.

[38] Above n 6, at p 44.

[39] Above n 6.

[40] Ibid, at p 136, see particularly Recommendations 4, 5 and 6.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

3.2 *The Technological Challenge: Data Banks and Data Mining*

There is a tendency for personal information to be accumulated in ever-larger data banks and some multi-billion dollar companies exist only for the purpose of collecting, analysing and sharing personal data with other companies.[41] One example is ChoicePoint, an American corporation that provides identification and credential verification services information to a large number of businesses and maintains information on a large number of individuals and businesses. Lax security safeguards on its part resulted in credit card information on some 40 million individuals being stolen in 2005 – an illustration of the harm that can result from such aggregated data banks if they are inadequately maintained.

Data matching between government agencies was the impetus for many of the early data protection laws.[42] The impersonal and possibly sinister implications for individuals (in particular the difficulty of challenging automated processes, the reversal of normal evidential presumptions and the potential for mistakes) led to the adoption of legislative safeguards such as those enacted in New Zealand[43] and Australia.[44]

In New Zealand, these safeguards provide for agreements between government agencies to be vetted beforehand by the Privacy Commissioner. The Information Matching Guidelines require the Commissioner to have regard to several factors, including cost-benefit considerations (whether the cost of the proposed programme is justified by the monetary or other benefits to society), whether alternative means exist for achieving the objectives sought and the principle of proportionality.[45] In addition, both legislative stipulations[46] as well as information matching rules promulgated under the Act[47] provide for such matters as technical standards, the destruction of data once it has been used against an individual[48] and procedural safeguards including prior notification to individuals before adverse action is taken against them. Time limits also exist for information matching programmes and the results of the programmes have to be reported annually to the Commissioner. These measures perhaps explain

[41] Ibid, at p 49.

[42] In New Zealand, for example, see the Privacy Commissioner Act 1991 which has been replaced by Part X Privacy Act 1993.

[43] Privacy Act 1993, Part X.

[44] Data-matching Program (Assistance and tax) Act 1990 (C'th). It should be noted that section 12 of this Act requires the Privacy Commissioner to issue Guidelines for the conduct of data-matching programmes and that a breach of either the Act or Guidelines constitutes an interference with privacy under s 13 of the Privacy Act 1988 (C'th) thus enabling a person to complain to the Privacy Commissioner.

[45] Privacy Act 1993, s 98.

[46] Ibid, Part X.

[47] Ibid, Fourth Schedule.

[48] In other words a further 'black list' of those caught cheating the social welfare for example cannot be maintained after the initial adverse action is taken against the individuals concerned.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

why information matching has become generally accepted by the public in New Zealand.

A further dimension to data matching is that it may occur between government agencies in more than one jurisdiction. This tendency is likely to become more prevalent. Again, the existing domestic safeguards are capable of addressing the issues that arise in this context. Under the New Zealand Guidelines, for example, agency-to-agency agreements must be scrutinised by the Commissioner and reported afterwards even where these involve data exchanges with overseas agencies.[49]

Data matching in the private sector is more problematic. Few jurisdictions outside Europe have adopted the stipulations of its Privacy Directive that require that an organisation must not make a decision adverse to an individual based on automated processing unless the individual has either consented beforehand or sufficient measures exist to safeguard the data subject's legitimate interests.[50] It has been seen that such safeguards, such as the right to notice before adverse action is taken and the right to challenge decisions concerning the data subject, exist thus far only in the public sector data matching programs of Australia and New Zealand.

In jurisdictions that have not adopted the European Privacy Directive's stipulations in this area, the existing privacy principles probably do not constitute an absolute bar to the practice of automated decisions concerning individuals by the private sector. However the requirements for transparency, consent and accountability mean that any such matching must be disclosed at the point of collection of the personal information as being a pertinent purpose for the information. Surreptitious matching would probably constitute a breach of the principles. Although it was not data matching in the strict sense there was still outrage, in New Zealand, when it was revealed that the Real Estate Institute had established a tenant database accessible to its members which collected data from landlords as to the 'tenant-worthiness' of up to 400,000 individuals (a sizable portion of New Zealand's population).[51] The better view is that, in the absence of a specific authorisation from the Privacy Commissioner, data matching ought not to occur apart from the governmental programmes sanctioned by legislation.

Far more insidious is the so-called practice of 'data mining'[52] that is being increasingly used post September 11. It involves extracting information from

[49] For example programmes between the New Zealand Inland Revenue Department and its Netherlands counterparts for the purposes of assessing eligibility for superannuation, pension and welfare payments was undertaken in the 2004-2005 year, see 'Annual Report of the Privacy Commissioner', (Wellington, 2005) at pp68-71.

[50] Above n 8, Article 15.

[51] 'Dangers of tenant database' *The New Zealand Herald* 10 January 2006.

[52] See W Renke 'Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy' (2006) 43 *Alberta LR* 779.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

large volumes of data and subjecting it to analysis, often using software that applies undisclosed and unverifiable analytical criteria and assumptions.[53] In the United States data mining has been described as:

> the application of database technology and techniques – such as statistical analysis and modelling – to uncover hidden patterns and subtle relationships in data and to infer rules that allow for the prediction of future results[54]

Privacy commentators have observed that an obvious feature of data mining is that the analysis of an individual's personal information creates new, secondary information about that person.[55] The privacy implications that arise include the fact that:

> The 'hidden patterns and subtle relationships' that data mining detects are recorded and become personal information of the individual…. Information about an individual's credit history, credit card purchases, law enforcement record or interactions, travel habits and so on may be mined to derive the finding that she is a possible terrorist who should be put on a terrorist watch list and kept under surveillance. This new personal information would become part of the swelling river of data whose channels are, in the private and public sectors, ever changing and difficult to follow, much less control. In this light data mining raises concerns about the accuracy and use of derived personal information, not to mention the individual's right of access to and correction of such information. [56]

The most ambitious use of data mining was undoubtedly the programme funded by the Pentagon in 2002 entitled the 'Total Information Awareness' project, a name later changed to the 'Terrorism Information Awareness' (TIA) in response to public concerns. The programme proposed to combine large amounts of information collected from the private sector into a giant database that would identify patterns believed to be associated with planning terrorist attacks.[57] Although funding for the research has been discontinued several agencies continue research into data mining and it has been reported that 52 United States federal agencies use or plan to use data mining, 'factual data analysis' or 'predictive analysis' in some 199 different efforts, of which at least 29 relate to detecting terrorist or criminal activities.[58]

---

[53] Above n 6, at p 51.

[54] US General Accounting Office, 'Data Mining: Federal Efforts Cover a Wide Range of Uses: Report to the Ranking Minority Member, Subcommittee on Financial Management, the Budget, and International Security', (Committee on Governmental Affairs, US Senate, May 2004) at p 1.

[55] Above n 6, at p 52.

[56] Ibid.

[57] Above n 6, at p 53.

[58] Above n 52, at p 789.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

The Computer Assisted Passenger Pre-screening System (CAPPS and its later version CAPPS II) also used data mining elements.[59] Although discontinued in its original form the CAPPS programme is currently entitled 'Secure Flight' but, as noted earlier, is still the source of ongoing controversy with the European Union. The controversy has been beneficial to privacy advocates. It has, for instance, been noted that while CAPPS II would have relied upon algorithms to predict whether a specific passenger was likely to be a terrorist, Secure flight, on the other hand, relies on checking passenger data against a centralised interagency terrorist watch list meaning that the program will only search for known or suspected terrorists.[60] Furthermore, the database is only available to the Transportation Safety Authority's personnel (as opposed to airline employees) whilst there now exists a 'redress mechanism, where people can resolve questions if they believe they have been unfairly or incorrectly selected for additional screening.'[61] Finally, another positive aspect is that unlike CAPPS II, Secure Flight does not extend to looking for those with outstanding warrants, such as those wanted for serious criminal offences, an expansion of law enforcement powers criticised as unnecessary for airline safety.[62]

The British Columbia Privacy Commissioner has recommended that his Government undertake an independent audit of data mining activities by all public bodies, identify and publicise such activities and develop legislative mechanisms for applying fair information practices to data mining.[63] In principle, there would seem to be no reason why data mining should be proscribed altogether. It may be, for example, that rules analogous to those enacted for data matching (discussed above) can be developed to allow the use of data mining provided its benefits can be demonstrably justified and that transparent monitoring and criteria are put in place. There may be a case for secrecy where aspects of security use are concerned[64] but no grounds for secrecy exist for other uses of data mining.

3.3 *The Security Challenge: A Trojan-Horse for Attacking Privacy?*

Proponents of privacy have had a particularly difficult time since the terror attacks of September 11, 2001. Governments in the United States and

[59] Ibid.

[60] J T Soma, MM Nichols, SD Rynerson, LA Maish & JD Rogers 'Balance of privacy vs security: a historical perspective of the USA PATRIOT Act' (2005) 31 *Rutgers Computer & Technology Law Journal* 285 at pp 343-344.

[61] Ibid.

[62] http://www.wired.com/news/privacy/0,1848,64748,00.html.

[63] Above n 6, Recommendation 10, p 138.

[64] The risks and alleged benefits of data mining are thoroughly examined by Renke, above n 52. Renke argues, convincingly, that extreme caution must be exercised before employing such technology given the fact that modern terrorist organisations do not exhibit the same traits as those which existed in the past and also differ in many significant ways from organised criminal organisations. Many assumptions on which data mining is founded may therefore be incorrect resulting in mistakes and consequent undermining of the public confidence in the efficacy of the practice.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

elsewhere have faced relatively little opposition in enacting measures that in many cases impinged seriously on personal privacy whilst at the same time curtailing existing privacy safeguards. These laws have been enacted with the ostensible goal of enhancing the public's security against terrorist and other threats.

Epitomising these measures is the American Patriot Act, an acronym standing for 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism' Act (Patriot Act) of 2001.[65] Its purpose was to amend and extend a number of United States laws and rules dealing with intelligence and counter-intelligence activities, information sharing and terrorism.[66] Detailed examination of the Patriot Act is outside the scope of the present discussion. It suffices, however, to make three observations about it.

First, section 215 amends the Foreign Intelligence Surveillance Act (FISA) which empowers the United States Foreign Intelligence Surveillance Court (FIS Court) to issue secret orders to enable the FBI to obtain records from third parties. Whereas previously orders could only be sought where the FBI could show specific facts giving reason to believe the person the records sought about was a foreign power or agent thereof, section 215 lowered the threshold to showing that records are sought for an authorized investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.[67]

Furthermore, whereas FISA orders were previously limited to certain business records held by public carriers and accommodation, physical storage or vehicle rental facilities, section 215 expanded the power to make orders to obtain 'any tangible thing' and removed the restriction on the kinds of organisations covered.[68] There has been much concern in the United States about these orders being presented to hospitals, libraries, bookstores, schools and all variety of businesses.[69] It has been contended that FISA orders may be made in relation to entire databases of information.[70]

Secondly other provisions of the Patriot Act have been almost as contentious. These include section 218 which altered the authority for physical searches and electronic surveillance under FISA: instead of requiring foreign intelligence to be 'the purpose' of the search or surveillance, it only needs to be 'a significant purpose.'[71] Section 505 in turn lowers the

[65] USA Patriot Act, Pub. L. No. 107-56, 115 Stat.272 (2001).
[66] Above n 6, at p 23.
[67] Above n 6, at p 70.
[68] Ibid.
[69] Ibid at p 71.
[70] Ibid.
[71] 50 U.S.C. SS 1804 (a) (7) (B) and 1823 (a) (7) (B); the United States courts have sanctioned the use of the powers for such expanded purposes, see for example *In re: Sealed Case* 310 F.3d 717 (U.S. Foreign Int. Surv. Ct. Rev. 2002) and *United States v Sattar* 2003 U.S. Dist. LEXIS 16164 (S.D.N.Y. 2003).

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

threshold for the FBI to issue orders under a number of statutes,[72] called 'national security letters' that compel financial institutions, phone companies and internet service providers to disclose information about their customers.[73] The threshold is merely 'relevance to an authorised intelligence investigation' and unlike orders issued by the FIS Court, national security letters are issued by the FBI directly, and secretly, without judicial supervision, the power being expanded to cover records held by travel agencies, real estate agents, the United States Postal service, jewellery stores, casinos and car dealerships.[74]

There are also provisions that encourage, rather than mandate, organisations to voluntarily report suspicious activities and purport to offer complete immunity against criminal and civil liability anywhere in the world for so doing.[75] These differ from conventional whistle-blower protection measures that are usually narrower in focus and set out specified channels for disclosure.[76] More insidious, however, are the recent revelations by the *New York Times* of secret schemes monitoring millions of bank records through accessing data from the Brussels-based Swift organisation[77] and its revelations in late 2005 of a warrant less eavesdropping programme ordered by the United States President.[78] These would appear to fall outside the ambit of any law altogether.[79]

The Patriot Act has obvious implications for individuals and businesses outside the United States as well. Apart from the outsourcing trends mentioned earlier, the law's reach extends to all United States registered corporations and their subsidiaries. As the case involving the money transfer company referred to earlier demonstrates, many large enterprises that operate outside the United States nevertheless transmit personal data to it

[72] 18 U.S.C. S 2709 (counterintelligence access to telephone toll and transactional records); 12 U.S.C. S 3414 (special procedures for financial records); 15 U.S.C. S 1681 u (credit record disclosures to FBI for counterintelligence purposes).

[73] Above n 6, at p 73.

[74] Ibid.

[75] For example see section 351, Patriot Act.

[76] For discussion of different approaches to whistle-blowing see G Gunasekara 'Whistle-blowing: New Zealand and UK Solutions to a Common Problem' (2003) 24 Stat LR 39.

[77] 'Bank Data Is Sifted by U.S. in Secret to Block Terror' *The New York Times* June 23, 2006.

[78] 'Bush Secretly Lifted Some Limits on Spying in U.S. After 9/11, Officials Say' *The New York Times* December 15, 2005.

[79] To be fair to the US Administration it did claim, in respect of the SWIFT disclosures, authority under the International Emergency Powers Act 50 U.S.C. ss 1701-1707 (1977), whilst at the same time arguing that privacy legislation, such as the Right to Financial Privacy Act 1978, applied to banks, not to a banking co-operative such as Swift. Furthermore the Admistration maintains the latter legislation applies to dealings between individuals and banks not to dealings between major institutions that route money through Swift on behalf of their customers. As to the basis for warrant less eavesdropping the Admistration appeared to rely on both Congressional resolutions on the campaign against terror as well as the argument that 'the Constitution vests in the President inherent authority to conduct warrant less intelligence surveillance of foreign powers or their agents.' Assessment of the merits of these claims is beyond the scope of this article and at least some of the Administration's actions are currently under review by the United States courts.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

for a variety of reasons. In all of these instances the Patriot Act and other United States laws will apply.

The United States legislative measures have had their counterparts in other jurisdictions for example in Canada[80] and in New Zealand.[81] While similar in many respects there are also significant differences, however. For example in New Zealand interception warrants must generally be issued by a judicial officer[82] and the right to access and correct information held by intelligence agencies is available.[83] Likewise complaints may be made to an independent judicial officer who is also charged with independent oversight over the activities of intelligence organisations.[84] The oversight over both the public and private sectors provided by the Privacy Commissioner which includes assessment of all new legislative measures impinging on privacy, also offers a measure of re-assurance. Despite this, New Zealand's legislative responses to the terrorist threat have still met with criticism.[85]

What are the privacy implications of these global trends? Several distinct issues can be identified. First, there is the tendency by Governments to co-opt the private sector into collecting personal information for purposes other than their own. The Canadian Privacy Commissioner has described this as:

> …deputizing the private sector organizations as law enforcement agents, and commandeering personal information that they have collected from individuals for entirely different reasons, in violation of the most basic fair information practices. [86]

One consequence has been that attempts, such as that of the Europeans, to 'quarantine' personal information relating to public security and defence from the application of privacy rules, are likely to be doomed from the outset.[87] The PNR dispute involving airlines is one example of this.[88] In this sense the American security focus represents a very real 'Trojan Horse' for attacking the European privacy fortress. It remains to be seen whether the Europeans can devise a new paradigm for resolving this conflict.

Secondly, a related development has been the blurring of the distinction between traditional law enforcement and counter-intelligence/terrorist operations. Higher thresholds and greater safeguards exist in respect

[80] Anti-terrorism Act, S.C. 2001, c. 41; Canadian Security Intelligence Service Act, R.S.C. 1985, C-23.

[81] Terrorism Suppression Act 2002, Financial Transactions Reporting Act 1996 and the New Zealand Security Intelligence Service Act 1969 (as amended).

[82] Commissioner of Security Warrants, required to have served as a High Court Judge, see Security Intelligence Service Act 1969 s 5A.

[83] Privacy Act s 57.

[84] Inspector General of Intelligence and Security Act 1996.

[85] See for instance Professor Matthew Palmer, 'Counter-Terrorism law' [2002] *NZLJ* 456.

[86] Above n 21 at p 14.

[87] Article 3(2).

[88] Above n 9.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

of day-to-day law enforcement than exist for covert security operations which, of necessity, demand greater alacrity as well as lower evidentiary and other thresholds. Although some spill over is always inevitable[89] the danger is that:

> …this new latitude permits foreign intelligence gathering tools, which offer less rigorous protections for individual rights and liberties than the investigative tools that apply to criminal law enforcement, to become backdoor tools of convenience for ordinary criminal law enforcement. [90]

Finally a perhaps unintended but very real threat to privacy is posed by the technological imperatives spawned by the new security measures. The history of previous developments has led one commentator to conclude that 'technology drives uses. Where there is a way there is a will.' [91]

The past is littered with examples that prove the validity of this assertion. A great many military applications have led to the development of civilian uses, mostly beneficial, that we now take for granted. These include the internet itself, GPS (global positioning system), microwave ovens and Velcro. Yesterday's cutting-edge military applications tend to become today's household applications of convenience.

The same must surely hold true for many of the experimental techniques such as data mining.[92] One danger is of such extraordinary technologies being used for non terrorist related law enforcement, so-called 'mission creep'. More alarming, however, will be the day when it is discovered that they are being routinely utilised by private sector firms to predict, say, patterns of consumer preference or risk-worthiness (particularly useful for insurance companies). The designers of software involved for security uses are likely eventually to take their wares elsewhere especially when their products are no longer used in the public sector.

There must therefore be no blanket exemptions for security-related applications from privacy norms. They are likely to be akin to the Trojan-Horse which once allowed within the city proved fatal to its liberty.

4 Jurisdictional Responses

4.1 *Restricting Exports of Personal Information*

From an early stage those formulating information privacy norms have been aware of the need to address the cross-border issue as witnessed by

[89] For example see the New Zealand Security Intelligence Act 1969 ss 4G & 4H (relating to the destruction of irrelevant records obtained by interception and the prevention or detection of serious crime).

[90] Above n 6 p 72.

[91] R Erickson & K Haggerty, *Policing the Risk Society* (University of Toronto Press: Toronto, 1997) at p34.

[92] See the discussion in the previous section.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

the OECD Guidelines. By far the most comprehensive attempt to address the issue, however, was undertaken by the European Union in the context of harmonising privacy rules amongst its members. A central pillar of its Privacy Directive, adopted in 1995, was that personal data could only be transferred from a Member state to a third country if the third country ensured an 'adequate' level of protection for the data after transfer.[93] Member states are required to prohibit the transfer of personal data where this requirement is not met. The Privacy Directive has been implemented in all the Member States of the European Union[94] and this requirement has effectively placed a fence around it in respect to the transfer of personal information. The obvious implications of this policy for trade and commerce with European Union countries did not go unnoticed and, as noted above, other jurisdictions including those in South America, Australasia and Asia have implemented privacy rules largely to meet the Privacy Directive's adequacy standard. Although trade has not to date been affected in the way initially feared and the Privacy Directive itself contains many exceptions,[95] jurisdictions have nevertheless sought to benchmark their privacy standards against those of the European Union which was seen as setting the world standard.[96]

The United States' refusal, from the outset, to adhere to the European privacy norms led to what was to become one of the most protracted of international disputes. The potential existed for the disruption of international trade, especially in services, between these giant trading blocs. Following lengthy negotiations[97] the European Union and the United States finally reached agreement, in March 2000, on a set of voluntary principles, known as the 'Safe Harbor Principles' which in due course received the approval of the European Commission as satisfying the adequacy requirement of the Privacy Directive.

The Safe Harbour Principles were issued by the United States Department of Commerce but are not mandatory, instead applying only to private firms that subscribe to them. However for those firms that do the principles are binding and penalties for non-compliance may be imposed by the US Department of Commerce.[98] As of June 2006 nearly 1000 organisations are listed as subscribing to the principles.[99]

---

[93] Article 25.

[94] See for example, in the United Kingdom, the Data Protection Act 1998 Schedule 1, Part I principle 8 and Schedule 1, Part II clause 13.

[95] Article 26: these include the consent of the data subject, contractual and other undertakings given by the transferee, matters considered further below.

[96] Heisenberg above n 35, at p 1.

[97] These are examined in detail by Heisenberg above n 35.

[98] United States Department of Commerce, *Issuance of Safe Harbor Principles and Transmission to European Commission*, 65 Fed Reg 45666 (2000).

[99] Available at: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list!OpenDocument&Start=976

Downloaded from https://academic.oup.com/jiplt/article/17/2/147/914150 by guest on 27 December 2020

Critics have noted that the Safe Harbor solution is more in line with the earlier OECD Guidelines than with the Privacy Directive.[100] As such it essentially preserves the fundamental differences between the European and American approaches to information privacy and is therefore far from ideal.[101] Significantly, however, other jurisdictions have not sought to emulate the United States approach or, perhaps more realistically, have not had the bargaining leverage to obtain their own safe harbour exemptions. Instead they have for the most part sought to obtain adequacy findings in their own right from the European Commission.

It is important to note that one of the pre-requisites for an adequacy finding by the European Commission is the degree to which the third country itself regulates the onward transfer of personal data. This is understandable as otherwise countries that themselves have adequate data protection regimes may simply be used as 'data havens' or as a conduit to other destinations, thereby circumventing the Privacy Directive.

Many jurisdictions have accordingly sought to adopt safeguards whilst at the same time allowing for the onward transfer of personal information – the core issue in the current discussion. For example, in Australia, Principle 9 of the National Privacy Principles provides for transfer of personal information in a number of circumstances.[102] These include the actual or implied consent of the data subject, the taking of 'reasonable steps' to ensure that the transferee will act consistently with the National Privacy Principles and where the transfer is necessary for the conclusion of or performance of a contract concluded in the interests of the data subject between the transferor and a third party.

However the ability to onward transfer personal data where companies 'reasonably believe' they are similarly protected in the third country has been criticised.[103] The criticism may be misplaced: Other jurisdictions have employed similar criteria, for example the equivalent provision in Hong Kong allows the onward transfer of personal data where the transferor 'has reasonable grounds for believing that there is in force in that place any law which is substantially similar to or serves the same purpose as this Ordinance.'[104] The European Privacy Directive itself allows derogations from its otherwise stringent provisions which are similar in their effect if not in their content.[105]

---

[100] D Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University LR* 131, at p 175.

[101] Ibid.

[102] Privacy Act 1988 (as amended) (C'th, Aust) Schedule 3, clause 9.

[103] Heisenberg above n 35, at p 110.

[104] Personal Data (Privacy) Ordinance No 81 of 1995 s 33.

[105] Article 26; one point of distinction is that, under the European provisions the onus is on the transferor to adduce 'sufficient safeguards' meaning that concrete steps are necessary on its part, another is that rigorous duties of notification exist where transfer occurs together with the right of the Commission and Member states to object to the transfer. Despite this, the experience with Safe Harbor has shown that the Europeans in effect adopt a 'reasonableness' test in deciding whether third countries ensure an 'adequate' level of protection for personal data.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

The exception allowed for contractual necessity (where the contract is between the data subject and the transferor the data subject's implied consent can also be argued) has also been subject to criticism.[106] Transfer is permitted of personal data where it is 'necessary for the performance of the contract' either between the individual and the transferor or between the transferor and a third party provided this is 'in the interests of" the individual.[107] How might necessity and the interests of the individual be assessed? This exception differs conceptually from other exceptions to privacy principles found elsewhere, for instance ones relating to health and safety or law enforcement. The latter involve balancing the interests of the individual against those of society as a whole. With contractual necessity, though, the economic interests of the individual must be assessed and balanced against the interests of the data controller. Potentially considerations of economic efficiency might be a factor. This is certainly relevant where cost-motivated offshore outsourcing decisions are made.[108] Presumably, though, the transferor would have to demonstrate a reason for the outsourcing other than avoiding complying with data protection rules.

Sanctioning the onward transfer of personal information on the basis of the actual or implied consent of the data subject is also subject to serious shortcomings. Consent has been described as 'ephemeral' (because it can always be withdrawn) and not a sound basis on which to build data processing practices.[109] In any event it is trite to say that informed consent is necessary. However consent cannot be truly informed unless the data subject is aware, at the outset, of all the downstream uses to which the information will be put making it difficult at least to use this as the basis for allowing the transfer of data overseas.

The circumstances where transfer of personal information abroad is sanctioned under these provisions may broadly be divided into two areas. First is where the transfer is in the context of an ongoing relationship between the data subject and the transferor or between the transferor and a third party in relation to the data subject. This relationship is likely to be based in contract but is certainly not confined to where a contract exists.

The second situation, however, is of greater interest. This is closer to where a true alienation or disposal of the personal data occurs. In this case the transferor divests itself of any continuing obligations, as far as complying with data protection principles is concerned, in relation to the personal data. The obligations, if any, are from that point onwards those of

[106] R Baker, 'Offshore IT Outsourcing and the 8th Data Protection Principle – legal and regulatory requirements with reference to Financial Services' (2006) 14 *International Journal of Law & Information Technology* 1 at p 11.

[107] The almost identical United Kingdom provision is found in the Data Protection Act 1998, Schedule 4, cl 3 c.f. Privacy Act 1988 (C'th, Aust) Schedule 3, cl 9.

[108] See Baker, above n 106, at p 11.

[109] Ibid.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

the transferee. Under the provisions discussed above the obligation of the transferor in these circumstances is to ensure either that the transferee is subject to a regime that is substantially similar to that of the transferor's own jurisdiction or that other measures are taken (such as contractual undertakings) to ensure that the personal data is dealt with in a manner consistent with the requirements of the transferor's jurisdiction.[110] What is sought is functional equivalence, not a rigid uniformity of rules.

These principles as to onward transfer are, of necessity, open-ended. They point to the imperative for proactive measures to be adopted in future to close any privacy loopholes and lead inexorably to cross-jurisdictional paradigms. Far from being a solution the existing jurisdictional approaches are therefore merely a pointer to future developments. It is precisely this hiatus that the present article seeks to address.

It should be said that the prevalence of the terms 'reasonable belief' or 'reasonable steps' is unsurprising. The reasonableness standard is commonly found throughout the privacy principles. For instance the requirement that information must be securely held is not an absolute standard: organisations must take 'reasonable steps' to protect the personal information they hold from misuse and loss and from unauthorised access, modification and disclosure.[111] In New Zealand they must protect information 'by such security safeguards as it is reasonable in the circumstances to take.'[112] Thus it is recognised that there is no failsafe guarantee against the determined hacker and so forth, what is sought is measures that are reasonable.

The concept of reasonableness is of course no stranger to the law. It an objective standard and is applied in many contexts including the determination of standards of care. When a holder of personal information transfers the data overseas the decision to do so must therefore be based on an objective belief that the data subject will continue to enjoy rights in relation to the information which are functionally equivalent to those enjoyed previously by the data subject. How this determination may be made is further explored below.

Some jurisdictions have as yet not addressed the onward transfer issue in their privacy regimes. In New Zealand, for example, there is recognition that this is a gap that must be addressed in order to ensure an adequacy finding from the European Union.[113] Limited application of extra-territorial provisions (discussed below) provides a partial solution but is inadequate on its own to resolve this issue.

[110] The US Safe Harbour scheme would presumably fall into the latter category.

[111] National Privacy Principle 4, Privacy Act 1988 (as amended) (C'th, Aust) Schedule 3, clause 4.

[112] Privacy Act 1993, s 6, Information Privacy Principle 5.

[113] See Office of the Privacy Commissioner, 'Necessary and Desirable: Privacy Act 1993 Review' (Wellington, 1998) Recommendation 35, at p 107.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

4.2 *Extra-territorial Application of Domestic Rules*

A different angle to the cross-jurisdictional dilemma and one that may, in the practical sense, be more useful, is the possibility for extra-territorial application of domestic privacy rules. Less contentious is the situation where domestic laws apply to an overseas entity that collects personal information about an individual when it operates within the domestic jurisdiction. Since trans-national businesses operate across several jurisdictions the issue is a very real one.

Jurisdictions have attempted to address this problem in different ways. There is much to be said for the Australian approach. The Act applies to conduct outside Australia if the information relates to an Australian citizen or resident and the organisation responsible for the conduct is either incorporated or has some other connection with Australia or carries on business in Australia.[114] Hence if an Australian company attempted to send personal data concerning Australians offshore for processing, it would not be able to avoid application of Australian law. Similarly, an overseas company that collected Australians' personal data would be caught by Australian law if the company was carrying on business in Australia and the information was collected in Australia. Presumably this would catch an overseas firm that advertised on the internet where the advertisement was accessible in Australia and the information was sent from Australia.[115]

On the other hand, a company unconnected with Australia that collected information relating to an Australian citizen, whilst he or she is outside Australia, would not be caught. This serves to illustrate the idiosyncratic and patchwork nature of the current data protection regime which depends on domestic enforcement of global privacy norms.

By comparison, the equivalent New Zealand provision is somewhat weaker although it arguably achieves the same result as its Australian counterpart. In the first place, access and correction rights apply even where a New Zealand agency holds information outside New Zealand.[116] When construed together with other provisions that impose obligations on the principal even where another conducts data processing on its behalf,[117] this would seem to cover the case of outsourcing.

Secondly, the main processing obligations (security, accuracy, use and disclosure for stipulated purposes) apply to any situation where personal information has been 'transferred out of New Zealand.'[118] This would

[114] Privacy Act 1988 (as amended) (C'th, Aust) s 5 B.

[115] The precise meaning of 'collected…in Australia' would need clarification. See also the discussion relating to the French case *of LICRA & UESF v Yahoo* Tribunal de Grande Instance de Paris No RG: 00/5308 and the other cases discussed by Judge David Harvey in *internet.law.nz* (2 ed., LexisNexis: Wellington 2005) at pp41-102.

[116] Privacy Act 1993 s 10(2).

[117] Ibid, s 3(4).

[118] Ibid, s 10(1).

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

accordingly include information collected from New Zealand by an overseas agency.[119] Likewise the main point of collection obligations (direct collection, the need to inform the data subject of intended purposes and recipients amongst others) would also apply to the overseas agency as it would be collecting the information in New Zealand.[120]

Nevertheless the privacy provisions in New Zealand are not in line with other legislation, such as the Fair Trading Act 1986, which clarify the issue of extra-territoriality.[121] The matter could be made unambiguous by the simple addition to the definition of 'agency' the stipulation that it:

> Includes an overseas agency that collects personal information in connection with the supply of goods or services in New Zealand or the carrying on of an activity in New Zealand

It should be noted that a further provision in the New Zealand legislation provides a defence for organisations once information has been transferred to another jurisdiction. This states that there is no breach of any of the information privacy principles in respect of any action that the agency is required to take by or under the law of any place outside New Zealand.[122] A similar provision in Australia stipulates that no interference with privacy will occur if the applicable law of a foreign country requires an act or practice.[123]

Although the existence of this defence is understandable in terms of sensitivities with regard to national sovereignty, it is nevertheless questionable as to whether it is justified. Companies and individuals should not be permitted to shelter behind it except where they can point to an unambiguous and mandatory stipulation of the foreign jurisdiction. Permissive stipulations such as those referred to earlier[124] certainly do not fall into this category. Whistle-blowing is another area that has occasioned difficulty.[125] Powers such as those of the FBI to issue national security letters discussed above are, of course, a different matter.

Even where the foreign law mandates certain conduct (including non-disclosure to the data subject of the action required by the foreign law) this will not apply at the point of collection in the domestic jurisdiction.

---

[119] It should be noted that 'agency' is given a broad definition encompassing both the private and public sectors and includes natural persons, bodies of persons and corporations; see Privacy Act 1993 s 2.

[120] It would fall within the definition of 'agency' as set out above.

[121] The applicability of this Act to conduct outside New Zealand is made clear by s 3 which stipulates: 'This Act extends to the engaging in conduct outside New Zealand by any person resident or carrying on business in New Zealand to the extent that such conduct relates to the supply of goods or services, or the granting of interests in land, within New Zealand.'

[122] Privacy Act 1993 s 10(3).

[123] Privacy Act 1988 (as amended) (C'th, Aust) s 13 D.

[124] Above n 75.

[125] See the discussion by M Schmidl, 'The Article 29 Working Party Opinion on Whistleblowing' (2006) 6 *World Data Protection Report* 23.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

Hence in the first example given at the outset of this article the individual should have been informed that, in order to process his money transfer, the information would have to be checked against international or United States lists of known terrorists for security vetting purposes. There is no reason why compliance with foreign law should not be inconsistent with complying with domestic rules as well. Say, for example, that an overseas law requires the information to be forwarded to the relevant taxation authority. If this was disclosed to the data subject at the outset or, subsequently authorised by him or her then, in most cases, no breach of domestic privacy rules will have occurred.[126] In a great many instances transparency is a complete cure with respect to alleged interferences with privacy.

Extra-territoriality is not, however, a panacea for dealing with many trans-border issues, particularly when domestic laws are inconsistent and possibly even clash with privacy values. Ultimately, alternative approaches are needed.

5 Analogous Solutions

I finally consider several solutions to address the difficulties outlined above. Some of these have already been implemented in certain jurisdictions; others are more in the nature of an exercise in brainstorming or considering solutions from other legal fields that may offer helpful analogies.

5.1 *Contractual / Property Paradigms*

It has been seen that several jurisdictions sanction the onward transfer of personal data where adequate contractual guarantees are elicited from the transferee of the data. Indeed by this means the data controller's entire gamut of privacy duties, in relation to the information, may be transferred to the recipient of the data.[127] The difficulty with contract is, of course, the doctrine of privity of contract meaning that a contract is only enforceable by the parties to it and not by third parties. This rule has been relaxed in most jurisdictions so that the clear beneficiary of a stipulation such as one for the benefit of a data subject can be enforced by the latter. [128] The difficulty still remains where information is further transferred, by the original transferee, to another party. An entirely new contract would be required with each subsequent transfer.

[126] In New Zealand for example see Privacy Act 1993 s 6, Information Privacy Principle 11(d).

[127] A schedule, for example, can easily be attached to the contract containing the Fair Information/Privacy Principles.

[128] In New Zealand, see Contracts (Privity) Act 1982.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

Property lawyers will, of course, recall that *Tulk v Moxhay*[129] established the doctrine that a restrictive covenant, binding a purchaser not to perform certain acts of ownership upon the land bought, may be enforced, not only against that purchaser as the contracting party, but also against third parties who later acquire the land.[130] The liability of the third party is based on both notice and the requirement that the covenantee must have retained other land in the neighbourhood for the benefit and protection of which the restrictive covenant was taken.[131] The question as to whether this equitable doctrine can be applied where the subject matter of the contract is other than land has exercised considerable judicial and academic controversy.[132]

In the old case of *De Mattos v Gibson* Knight Bruce LJ asserted, in relation to charter rights over a ship that:

> Reason and justice seem to prescribe that, at least as a general rule, where a man by gift or purchase, acquires property from another, with knowledge of a previous contract, lawfully and for valuable consideration made by him with a third person, to use and employ the property for a particular purpose in a specified manner, the acquirer shall not, to the material damage of the third person, in opposition to the contract and inconsistently with it use and employ the property in a manner not allowable to the giver or seller. [133]

Despite being applied by the Privy Council in a subsequent case[134] this sweeping principle has not been universally applied outside the sphere of restrictive covenants in relation to land and subsequent cases have narrowed it to limited circumstances.[135] The difficulty is that there is no proprietary interest retained by the covenantee.[136] Other solutions suggested include those of holding the subsequent purchaser to be a constructive trustee or invoking the tort of inducing breach of contract.[137] It has also been questioned whether any remedy can extend beyond the grant of a negative injunction as opposed to a positive order to perform the contract or an award of damages.[138] This would have obvious ramification in relation to personal information, for instance where access to information or correction of it was sought or where damages are sought for a subsequent

---

[129] (1848) 2 Ph 774.

[130] Burrows, Finn & Todd, *Law of Contract in New Zealand* (2 ed., LexisNexis: Wellington 2004) at p 541.

[131] Ibid; see *London County Council v Allen* [1914] 3 KB 642.

[132] See S Gardner, 'The Proprietary Effect of Contractual Obligations under *Tulk v Moxhay* and *De Mattos v Gibson*' (1982) 98 *LQR* 279.

[133] (1858) 4 De G & J 276, 282.

[134] *Lord Stathcona SS Co v Dominion Coal Co* [1926] AC 108.

[135] *Port Line Ltd v Ben Line Steamers Ltd* [1958] 2 QB 146.

[136] Burrows, Finn & Todd, above n 130, at p 543.

[137] *Swiss Bank Corp v Lloyds Bank Ltd* [1979] Ch 548, 575 per Browne-Wilkinson J.

[138] Burrows, Finn & Todd, above n 130 at p 545.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

disclosure or use of the information that was inconsistent with fair information principles.

In the case of personal information does a company retain any interest after it sells personal data to another company? An argument may be made that it does. Certainly, from an economic standpoint the company stands to lose customer goodwill where it has parted with customer information and is unable to subsequently ensure it is not misused. From the legal standpoint the case may also be made that where the contractual assurances sought were not 'reasonable' the company may face legal sanctions under the data subject's privacy laws.[139]

These interests are not 'proprietary' interests in the conventional sense but ought, if a modern interpretation is taken of the existing principles outlined above, apply to this situation. Furthermore, data subjects themselves have interests in their personal information after it has been on sold or transferred to third parties. Data subjects' interests are not the information itself but the consequences that can occur from the use or misuse it.[140] In this regard they are analogous to land owners for whose benefit restrictive covenants were given.

Whether or not courts adopt such an approach the ability of data subjects to use contract to secure their information privacy rights is likely to be limited in scope. Conflict of law rules and the difficulty of litigating rights across jurisdictions with its attendant costs will always be a significant obstacle. It must be remembered that many information privacy regimes provide cheap dispute resolution mechanisms as an alternative to expensive litigation. Breaches of contract, on the other hand, must generally be litigated in the civil courts, except where arbitration is specified.

One option in developing a 'Fourth Generation' of privacy principles may be to allow national data protection authorities the power to enforce contractual stipulations or deem contravention of them to be a breach of privacy rules. Some jurisdictions already have provisions of this nature.[141] Another might be to require registration of such contractual clauses so that subsequent purchasers are put on notice, actual or constructive, as to the data subject's rights. It should be possible to attach a symbol such as the '©' symbol for copyright or abbreviations used in commerce such as 'cif' and the like. Perhaps the 'p' symbol might delineate the fact that standard privacy rights are covenanted in relation to information concerning the subject. Another requirement should be that the initial 'privacy

[139] See the discussion above relating to jurisdictional approaches towards restricting exports of personal information.

[140] For example denial of credit, health insurance or the ability to access air travel to name a few.

[141] Privacy Act 1988 (as amended) (C'th, Aust) ss 6 A(2), 6 B(2) & 13 A(c): service providers contracted to the Commonwealth government are bound by the terms of their contract where this is inconsistent with the privacy principles. A breach of contract is deemed to be a breach of the privacy principles in these circumstances.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

statement' given to an individual be attached to any subsequent transfer of the data: third parties will then be unable to claim that they received the information in ignorance of its intended uses and recipients.

Such measures may go some way towards addressing criticism of the use of contractual paradigms as a substitute for genuine adequacy assessment at the point of transfer or as a substitute for genuine regulatory monitoring of the process of cross-border transfer.[142] It has been rightly pointed out, however, that 'Model contracts are "the only show in town"' at present for offshore out-sourcing partly as a result of the inconsistent manner in which national data Protection authorities handle the issue of assessing adequacy on the part of the third country's data protection regime (some such as those of France and Austria, require a prior approval process prior to the export of the personal data whereas others carry out a post facto review).[143]

While the propensity for data controllers to hide behind a 'reasonable efforts' requirement is seen as something of a soft option[144] there is, at the same time, appreciation of the beneficial potential of the use of standard form contracts incorporating data protection standards, especially for multi-national companies that are subject to public scrutiny and regulation across frontiers.[145] Companies such as British Petroleum, for instance, adhere to both the United Kingdom Data Protection Act 1998 as well as to the European Privacy Directive.[146] Since it operates in many jurisdictions worldwide, this has the effect of bestowing the high European privacy standards on its employees and customers, even in jurisdictions where a lower privacy standard applies.

Despite criticisms of contractual approaches, the suggestions made in this article ought, if adopted, militate against potential dilution of data controllers' responsibilities when the contractual road is taken as the preferred option. A half-way house between existing solutions (rigid policing by national Data Protection Authorities or reliance on contractual mechanisms alone) is also proposed below.

5.2 *Consumer Law Model*

Another area that provides a useful source of analogy is that of consumer law. Most jurisdictions have consumer protection laws and fair trading laws designed to protect consumers from corporate excesses. Product safety and information standards are commonplace.[147] A theme running

[142] See Baker, above n 106 at p 10.
[143] Ibid, at pp 10, 25.
[144] Ibid, at p 13.
[145] Ibid, at p 14.
[146] See: http://www.bp.com/popuppreviewtwocol.do?categoryId=438&contentId=2008122.
[147] See for example Trade Practices Act 1974 (C'th, Aust) Part V Division 1 A and Fair Trading Act (NZ) Parts 2 & 3.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

through many of these is transparency as to the quality of the goods or services being offered. In this respect similarities exist with the fair information/privacy principles discussed above.

Fair trading laws also often allow for industry codes, binding or otherwise, to be adopted.[148] In this regard they are similar to privacy regimes which allow data protection authorities to modify rules or to promulgate rules for a particular sector with special needs such as for instance health care.[149] Ultimately it can be argued that there is little distinction between consumer rights and privacy rights – both usually require information disclosure and transparency and proscribe misleading or deceptive practices. This may be one way in which the reluctance of some jurisdictions, notably the United States, to adopt blanket information privacy rules may be addressed. From a business standpoint the advantage of a uniform set of standards is of course that of the level playing field – all business entities are equally subject to the same compliance costs.

Yet another model for cross-border transfer is the Cartagena Biosafety Protocol which is in force in its signatory countries (which include Australia and New Zealand).[150] This imposes rules with regard to food labelling and the like with regard to its genetically modified content. Although conceptually different to privacy (the duty is imposed on exporting countries to notify the degree of genetically modified content) the similarity is that the strictest importing jurisdiction's standard has tended to be the industry standard. There are obvious parallels with the Privacy Directive here.

5.3 *Corporate Law Solutions*

The business law models need not be confined to consumer law. Businesses increasingly deal across borders and must comply with numerous business law regimes in the jurisdictions in which they operate. This includes the like of Sarbanes-Oxley[151] in the United States. Corporate law also provides many analogies. For example publicly listed companies must be transparent in their information practices and most jurisdictions outlaw insider dealing. There is no reason why personal information should be treated differently.

Another common feature is the need for external audits of corporate practices. Organisations should also be periodically audited for their information practices. At present, companies must be audited for their financial practices. This task is undertaken, for the most part, by private

[148] See for example Trade Practices Act 1974 (C'th, Aust) Part IV B Industry Codes.

[149] In New Zealand see for instance the Health Information Privacy Code 1994.

[150] Cartagena Protocol on Biosafety to the Convention on Biological Diversity (adopted in May 2000) Articles 8 & 20.

[151] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat.745 (2002).

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

sector firms that specialise in the practice. Despite failures associated with the corporate collapses at the beginning of this century[152] the practice of private sector auditing has continued although with greater oversight by regulatory authorities. There is no reason why this cannot be paralleled in the personal data sphere. Providing it is sanctioned by regulation, this is an industry waiting to be born or still in its infancy.

Special audit arrangements should be set up with regard to the transfer of information across borders. In this regard analogies may be drawn with existing models where more stringent safeguards exist. For instance it has been observed that, in the United Kingdom, the procedures mandated by the Financial Services Regulator significantly exceed those of the Data protection Authority.[153] These require, amongst other things, that the adequacy assessments are carried out, documented and that they are retained for inspection by all financial services organisations.[154] If adopted, such a paradigm may represent a half way house between the approach of some Data Protection authorities that carry out a prior approval process prior to sanctioning personal data exports and others that carry out monitoring after the exports have occurred. Audits should also be carried out of the adequacy of standard contractual clauses – once again this is a task that can properly be entrusted to private sector specialists, such as law firms.

Companies also have periodic reporting obligations. Not only must they report to registry offices but reports must from time to time be compiled on compliance with health and safety and a myriad other regulations. Compliance with data protection rules ought to be subject to similar reporting obligations. In this regard the onus is on national Data Protection authorities to formulate simple yet functional forms (most forms can be downloaded through the internet nowadays) that data controllers must return at least annually. Such forms can incorporate boxes asking questions such as 'is customer data sent overseas' which must be ticked and returned as appropriate.

Self-certification is a theme running through many corporate governance rules. For example company directors in New Zealand are required to sign certificates attesting to a range of matters, ranging from the fairness of their own remuneration, the solvency of the company and the fairness to shareholders of various actions including the issuing of shares, share re-purchases by companies and payment of dividends. Not only may failure to comply with such requirements amount to a criminal offence and lead to potential civil liability on the part of the directors themselves, but, in addition, it allows shareholders to bring an automatic action for prejudicial conduct.[155]

---

[152] Such as the Enron debacle.
[153] See Baker, above n 106, at p 10.
[154] Ibid.
[155] Companies Act 1993 s 175(2).

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

These provisions ought to be emulated in respect to the duties of data controllers. Many data protection regimes require designated persons to be appointed, within an organisation, to deal with personal data issues.[156] It may be unreasonable to impose personal liability on these individuals themselves for lapses by them in relation to their obligations. However it is perfectly reasonable to pin any such lapses on their employers and the failure to sign a certificate of adequacy or similar requirement should automatically be deemed an infringement of data protection rules. It is important to state that self-certification, in this context, is not a substitute for external assessment of compliance with privacy standards. Rather, it is a mechanism for establishing liability on those who are found to have issued certificates without any reasonable basis.

The imperatives underlying health and safety initiatives also underlie much of the basis for data protection. Consumer awareness and education, although vital, are not themselves a substitute for self-monitoring and reporting by data controllers. Heisenberg points out that, in 2003, 68 percent of European citizens had never heard of the independent authorities that existed to hear consumer complaints.[157] Similarly, consumers might expect their health and safety to be safeguarded but do not necessarily believe enforcement of these standards is up to them.

Of course businesses are likely to baulk at the cost of yet another regulatory imposition. The benefits to business of having transparent information-handling mechanisms which reduce the likelihood of customer complaints and litigation must be factored into any cost-benefit analysis in responding to such criticism. Research has shown that customers place great value in an organisation's privacy safeguards. A UMR survey of public opinion in New Zealand in 2006 found that 93 percent of respondents considered good privacy practices by business as important as efficiency, and product quality, and service, and more important than convenience.[158] European and American studies have also consistently shown that citizens believe that governments are best placed to regulate and monitor compliance with privacy standards.[159] Business can therefore only benefit in the long term from more stringent privacy rules with regard to cross-border information transfers.

5.4 *International Solutions*

There has thus far been reluctance to formulate international regimes with regard to privacy apart from the original United Nations declarations

[156] Privacy Act 1993 (NZ) s 23.

[157] Heisenberg above n 35 at p 171.

[158] Quoted in Address by Marie Shroff, Privacy Commissioner 'Privacy and the consumer' Privacy Issues Forum, Wellington, 30 March 2006.

[159] See the studies catalogued by Heisenberg above n 35 at pp 37-40.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

on civil and human rights.[160] Some regional efforts have been made, especially in the Asia-Pacific region[161] and of course the most advanced international system is that of the European Union.

One option would be for an international privacy regime that would apply in the absence of 'substantially similar' domestic legislation. Conceivably an 'International Privacy Commissioner' may be set up. However enforcement would be problematic where a jurisdiction has not subscribed to such a mechanism. It may, of course, be possible to set up an international 'Safe Harbor' modelled on the United States solution but, again, enforcement would be the key problem.

International agreements do already operate to harmonize personal data handling practices in regard to some sectors. For example a new Recommended Practice concerning PNR data was included in Annex 9 (Facilitation) to the Convention on International Civil Aviation ('Chicago Convention') after being adopted by the International Civil Aviation Organisation (ICAO) Council in March 2005.[162] The practice requires Contracting states to conform their PNR data processing to guidelines developed by the ICAO.

In principle there is no reason why binding international treaties cannot be adopted in relation to the protection of information privacy. Intellectual property has witnessed such treatment[163] and there is much in common as personal information, like all information, shares characteristics including the ease of copying and transmission.

One area where international co-operation would be particularly useful is that of information sharing and technical exchanges between national Data Protection authorities. Such exchanges are common in other areas, for instance the Cartagena Protocol mentioned above establishes a Biosafety Clearing-House for the exchange of scientific, technical, environmental and legal information between participating countries.[164] Amongst other things the Clearing-House is to make available risk assessments and reviews and to assist developing countries to implement the Protocol.[165]

---

[160] See Article 12 of the United Nations Declaration of Human Rights and Article 17 of the International Covenant on Civil and Political Rights.

[161] See for instance the APEC Privacy Framework, available at: http://www.apecsec.org.sg/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html, the standards contained in it do not match those of the EU however as it fails, for example, to include any provisions relating to data exports.

[162] See R Abeyratne 'The use of information contained in the airline passenger name record – some issues' (2005) 10 *Communications Law* 170.

[163] For example the TRIPS agreement.

[164] Above n 150, Article 20.

[165] Ibid.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

Tentative moves in this direction have already been made in the privacy area. For example the Montreux Declaration of Privacy Commissioners states that they agree 'to create a permanent website …as a common base for information.'[166] In the Asia-Pacific region the *Privacy Law Project* under the auspices of the Cyberspace Law and policy Centre at the University of New South Wales, is developing a privacy database of global significance.[167] Collaboration in this area between the private sector, academic institutions and national Data Protection authorities ought to be encouraged.

6 Conclusion

This article has traversed several issues in the development of principles concerning the handling of personal data and the threats to these rules that arise from the flow of personal data across borders. These have been in the areas of trans-border business, technological development and security applications. The resulting undermining of core privacy safeguards has been very real and cannot be understated.

Despite this, a new 'fence' to tackle these challenges can be constructed; the task is not altogether hopeless. Many analogies exist in the corporate and governmental spheres that can be adopted. Consumer rights and transparency underlie much business regulation. These concepts can easily be extended to the privacy sphere. Likewise many of the safeguards adopted in respect to Governmental uses of personal data, for example data-matching between public agencies, are equally relevant to private sector applications and new phenomena such as data mining. Freedom of information laws that require transparency in Government use of information generally also provide a source of comfort to privacy advocates.

Good privacy regulation must not only put up fences but also track the movement of information through gateways to their final destination. In other words it is the exceptions that must be most rigorously monitored. It has been seen, for example, how information-matching between government agencies in New Zealand and elsewhere has been counterbalanced by setting up stringent safeguards as to reporting and frequent audits of the measures including cost-benefit analysis of the results. These measures can easily be transplanted elsewhere. The 'seamless' nature of information has been a two-edged sword because threats to personal information span public and private sectors. However there is no reason, in principle, why public sector solutions cannot be applied to the private sector and vice versa.

[166] 16 September, 2005 available at: http://www.libertysecurity.org/article709.html.
[167] Available at: http://www.bakercyberlawcentre.org/ipp/.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020

It should in theory be possible to develop a new generation of privacy safeguards especially in order to deal with the issue of cross-border transmission of personal information. The challenge in developing a 'fourth generation' set of protocols to regulate trans-border data flows will be to preserve the existing body of principles, now largely settled, that govern the collection, use and disposal of personal information.

Downloaded from https://academic.oup.com/jilit/article/17/2/147/914150 by guest on 27 December 2020