IS THERE A BETTER OPTION THAN THE DATA TRANSFER MODEL TO PROTECT DATA PRIVACY?

ALAN TOY* AND GEHAN GUNASEKARA**

The data transfer model and the accountability model, which are the dominant models for protecting the data privacy rights of citizens, have begun to present significant difficulties in regulating the online and increasingly transnational business environment. Global organisations take advantage of forum selection clauses and choice of law clauses and attention is diverted toward the data transfer model and the accountability model as a means of data privacy protection but it is impossible to have confidence that the data privacy rights of citizens are adequately protected given well known revelations regarding surveillance and the rise of technologies such as cloud computing. But forum selection and choice of law clauses no longer have the force they once seemed to have and this opens the possibility that extraterritorial jurisdiction may provide a supplementary conceptual basis for championing data privacy in the globalised context of the Internet. This article examines the current basis for extraterritorial application of data privacy laws and suggests a test for increasing their relevance.

I INTRODUCTION

The Internet and the growth of global business represent an existential threat to the ability of domestic data privacy laws to protect individuals who are just as likely to send their personal data to overseas entities as to those within their own jurisdictions.[1] The two principal approaches of data privacy laws to regulating such cross-border data transfers have been export prohibition or restrictions (the

* Senior Lecturer in the Department of Commercial Law at the University of Auckland Business School.
** Associate Professor in the Department of Commercial Law at the University of Auckland Business School.

1 'Since the Internet is structured to transit data based not on geography but on technical parameters … it may no longer be feasible to differentiate between transborder data flows and those that do not cross national borders': Christopher Kuner, *Transborder Data Flows and Data Privacy Law* (Oxford University Press, 2013) 6. See also the examples given by said author in chapter 1 as to the exponential growth of data transfers driven by technological developments.

data transfer model)[2] and, in the case of transfers by domestic actors, accountability for the data that is transferred (the accountability model).[3] It should be noted that there has been some agreement at the international level regarding data transfer and accountability mechanisms that could be relevant across different countries. Such initiatives come from the Organisation for Economic Co-operation and Development ('OECD') in the 2013 revision of the OECD privacy guidelines,[4] and the Asia-Pacific Economic Cooperation ('APEC') which established a Cross-Border Privacy Enforcement Arrangement in 2010.[5] But these initiatives have not yet been widely adopted.

The data transfer model and the accountability model are no longer adequate and the *Maximillian Schrems v Data Protection Commissioner* ('*Schrems*')[6] ruling, which invalidated the *Commission Decision 2000/520/EC of 26 July 2000*[7] giving rise to the uncertain[8] European Union-United States Privacy Shield, demonstrates that the export restriction approach is not sufficient on its own for protecting the privacy of European Union ('EU') citizens or, for that matter, citizens of any other jurisdiction. The Cambridge Analytica data scandal[9] also indicates that current approaches are insufficient. This article therefore makes the case for the third regulatory leg, consisting of limited application of domestic laws extraterritorially, which is rapidly emerging as an additional solution. It argues citizens should be able to complain to their relevant local Data Protection Authority ('DPA') under extraterritoriality provisions in local legislation and proposes a test to legitimise this whilst filtering out the unreasonable extension of such provisions. While this test may require legislative amendment to be applied in any country that wishes to adopt it, it does not require the agreement of states on a treaty governing data privacy (nor does it require that multiple countries adopt it) and is therefore a robust solution in addition to the other existing approaches. Whilst other potential models may yet emerge – such as technological ones – the three mentioned above are currently the principal approaches.

---

2 See, eg, *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* [1995] OJ L 281/31 art 25 ('*Directive 95/46*'), which has now been superseded by *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 art 45 ('*GDPR*').

3 See, eg, *Privacy Act 1988* (Cth) s 16C.

4 Lee A Bygrave, *Data Privacy Law: An International Perspective* (Oxford University Press, 2014) 47–9.

5 Ibid 78.

6 (Court of Justice of the European Union, C-362/14, 6 October 2015).

7 *Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the US Department of Commerce* [2000] OJ L 215/7.

8 Erika Morphy, 'Are You Ready for the End of Privacy Shield?', *CMS Wire* (online), 2 October 2018 <https://www.cmswire.com/content-strategy/are-you-ready-for-the-end-of-privacy-shield/>.

9 Kevin Granville, 'Facebook and Cambridge Analytica: What You Need to Know as Fallout Widens', *The New York Times* (online), 19 March 2018 <https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html>.

Clarity is first needed, however, as to what constitutes the exercise of extraterritorial jurisdiction.[10] It may be said to occur where states extend their adjudicative and prescriptive regulatory competence to persons outside their enforcement jurisdiction[11] whose conduct either emanates from within their territory or has effects within their territory. Professor Svantesson has argued that the phenomenon of cloud computing makes it problematic to identify the location of activities, proposing instead the following definition:

> an assertion of jurisdiction is extraterritorial as soon as it seeks to control or otherwise directly affect the activities of an object (person, business, etc) outside the territory of the State making the assertion – persons, whether legal or natural, are always located somewhere, while locating 'activities' is much more difficult.[12]

One such example may be found in the United States *Children's Online Privacy Protection Act of 1998*[13] which applies to websites anywhere in the world that collect personal information from children in the United States including those run from outside the United States but directed at children in the United States.[14]

A robust test for extraterritorial application of data privacy laws has not yet gained acceptance even as a supplementary method for safeguarding the data privacy rights of citizens. The reason for this may have to do with forum selection and choice of law clauses in online contracts which may have obfuscated the relevance of extraterritorial jurisdiction in the past. Recent rulings[15] are beginning to bring coherence to this issue with the denial of enforceability of a number of such clauses. This indicates that the imperative for extraterritorial jurisdiction of data privacy laws is gaining strength.

This article suggests a test to determine in what circumstances should the DPA or the local courts[16] have extraterritorial jurisdiction over data controllers.

---

10 It is not useful to classify this as an issue of purely civil law or of private as opposed to public international law. The common law has not arrived at a clear definition of public and private laws: Paul Torremans (ed), *Cheshire, North & Fawcett: Private International Law* (Oxford University Press, 15th ed, 2017) 123. Indeed, it has been argued that the distinction between public international law and private international law/conflict of laws has been 'eroded … into analytical uselessness': Anthony J Colangelo, 'What is Extraterritorial Jurisdiction?' (2014) 99 *Cornell Law Review* 1303, 1349.

11 Prescriptive jurisdiction is the 'power to make and apply law to persons or things' while adjudicative jurisdiction is the power to 'subject persons or things to judicial process' and enforcement jurisdiction is the power to 'induce or compel compliance or to punish non-compliance': Colangelo, above n 10, 1310–11.

12 Dan Jerker B Svantesson, *Extraterritoriality in Data Privacy Law* (Ex Tuto Publishing, 2013) 85.

13 15 USC §§ 6501–6 (1998).

14 See discussion in Svantesson, *Extraterritoriality in Data Privacy Law*, above n 12, 148.

15 See, eg, *Douez v Facebook Inc* [2017] 1 SCR 751 ('*Douez*'); *Verein für Konsumenteninformation v Amazon EU Sàrl* (Court of Justice of the European Union, C-191/15, 28 July 2016) ('*VKI v Amazon*'), which are discussed in Part V of this article.

16 In Australia, the Australian Information Commissioner or the affected individual may apply to enforce a determination of the Commissioner in the Federal Court or the Federal Circuit Court under s 55A of the *Privacy Act 1988* (Cth) and the hearing will be de novo. In New Zealand, following an investigation by the Privacy Commissioner, the Director of Human Rights Proceedings or the affected individual may bring proceedings under ss 82–3 of the *Privacy Act 1993* (NZ) in the Human Rights Review Tribunal in respect of an interference with the privacy of the individual. There are therefore situations in which the local DPA or the local courts may require extraterritorial jurisdiction.

The test proposed is that where an organisation (data controller/processor) conducts business or activities in the location of the data subject and where the privacy interests of the data subject have been prejudiced in that place, then the data privacy laws in force in the place of the data subject could properly apply to the data controller. The test being put forward recognises legitimacy of extraterritorial applications of data privacy laws but at the same time limits the scope of extraterritoriality and is thus consistent with goals of the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data of not restricting the flow of personal data.[17] The test proposed is applicable to non-state actors. Consideration as to the extent to which exceptions to the doctrine of sovereign immunity may permit claims in domestic fora against foreign governments is beyond the scope of this article and there is as yet no internationally agreed consensus, for example, as to the relationship between the intelligence gathering paradigm and data privacy rights.[18]

II THE SEARCH FOR A NEW MODEL

Increasing technological threats to privacy have arisen, such as the possibility of cross-device tracking technology.[19] One possible response to the challenges to privacy presented by new technologies is to simply surrender. This is certainly the attitude of '[i]nternet separatists … [who] seek to disable states from protecting their citizens online'.[20] However, such an attitude is deeply unsatisfying. A stronger argument is that consumers no longer have the same conception of privacy as they have had in the past.[21] While it may be arguable that conceptions of privacy have evolved, it cannot be concluded that they have become extinct. It is rumoured that the Trump Administration may be supportive of a Federal Online Privacy Bill,[22] although such efforts are as yet inchoate compared to those of the former Obama Administration, which released draft legislation intended to 'secure consumers' privacy through comprehensive standards and to create a level playing field across technology sectors.[23] In

17 Organisation for Economic Co-operation and Development, 'The OECD Privacy Framework' (Report, 2013) 16 [17].

18 International Working Group on Data Protection in Telecommunications, 'Towards International Principles or Instruments to Govern Intelligence Gathering' (Working Paper 675.54.10, 24–5 April 2017) <https://www.datenschutz-berlin.de/fileadmin/user_upload/pdf/publikationen/working-paper/2017/2017-IWGDPT_Working_Paper_Govern_Intelligence_Gathering-en.pdf>.

19 Federal Trade Commission, 'Cross-Device Tracking: An FTC Staff Report' (Report, January 2017).

20 Joel R Reidenberg, 'Technology and Internet Jurisdiction' (2005) 153 *University of Pennsylvania Law Review* 1951, 1953.

21 See Alan Toy, 'Generating Standards for Privacy Audits: Theoretical Bases from Two Disciplines' (2017) 25 *Journal of Law, Information and Science* 26, 46–7.

22 See, eg, 'Senate Commerce Committee Members Rumored to be Discussing Online Privacy Bill' on Hunton Andrews Kurth, *Privacy & Information Security Law Blog: Global Privacy and Cybersecurity Law Updates and Analysis* (31 August 2018) <https://www.huntonprivacyblog.com/2018/08/31/senate-commerce-committee-members-rumored-discussing-online-privacy-bill/>.

23 The White House, 'Privacy in our Digital Lives: Protecting Individuals and Promoting Innovation' (2017) (Report, January 2017) 2 <https://iapp.org/resources/article/privacy-in-our-digital-lives-protecting-individuals-and-promoting-innovation/>.

addition, President Obama has stated that 'even though we live in a world in which we share personal information more freely than in the past, we must reject the conclusion that privacy is an outmoded value'.[24] Accordingly, privacy protections facilitate the digital economy through building trust in online technologies.

Approaches to jurisdiction in respect of online activity have been developing in the context of the tort of defamation. In *Dow Jones & Co Inc v Gutnick* ('*Gutnick*'),[25] Mr Gutnick was able to sue in the Victorian courts in respect of a defamatory statement made by Dow Jones & Company Inc on an American subscription website. Mr Gutnick lived in Victoria and had his business headquarters there and while he did conduct some business abroad, including in the United States, 'much of his social and business life could be said to be focused in Victoria'.[26] While the case seemed to allow for potential liability in multiple locations, this possibility should not be overstated. If a person has few connections with a particular jurisdiction then it may be a challenge to show that their reputation has been negatively impacted in that jurisdiction. The principle in the case may be seen as an early and unsophisticated response to the issue of jurisdiction in respect of online activity. It is therefore relevant to data privacy but refinement of the principle has now occurred.

In *Bolagsupplysningen OÜ and Ingrid Ilsjan v Svensk Handel AB* ('*Ilsjan*'), which was also in the context of defamation, the search for a model that can apply to online conduct has moved in the direction of finding the 'centre of interests' of the complainant, which is where the conduct will be 'felt most keenly'.[27] This 'centre of interests', rather than all the places where online material may be available in the world, is the place in which the complainant can bring legal action in respect of 'all the damage sustained'.[28] It has been argued that the complainant should not be able to bring action in the courts of all the possible places in which damage has been suffered, as '[t]hat way madness lies'.[29] Although the case concerned defamation, which is only tangentially related to data privacy, the Court's analysis nonetheless supports the premise of this article. The Court, citing previous authority,[30] stated that

> the criterion of the centre of interests accords with the aim of predictability of the rules governing jurisdiction, since it allows both the applicant easily to identify the court in which he may sue and the defendant reasonably to foresee before which court he may be sued.[31]

---

24 Ibid 17.

25 (2002) 210 CLR 575.

26 Ibid 594 [2] (Gleeson CJ, McHugh, Gummow and Hayne JJ).

27 *Ilsjan* (Court of Justice of the European Union, C-194/16, 17 October 2017) [33] (The Court).

28 Ibid [44] (The Court).

29 Andres Guadamuz, 'CJEU Ruling on Internet Jurisdiction' [2017–18] (December/January) *Computers & Law* 3, 3.

30 *eDate Advertising v Olivier Martinez* (C-509/09 and C-171/10) [2011] ECR I-10269, I-10322 [50] (The Court) ('*eDate*'), cited in *Ilsjan* (Court of Justice of the European Union, C-194/16, 17 October 2017) [35] (The Court).

31 *Ilsjan* (Court of Justice of the European Union, C-194/16, 17 October 2017) [35] (The Court).

The Court noted, furthermore, that the criterion is intended to determine the place in which damage caused by online content occurs and, consequently, the Member State whose courts are best able to hear and rule upon the dispute. Although at the same time noting in matters relating to tort, delict or quasi-delict that the rule of 'special jurisdiction' must be interpreted in line with the 'scheme and purpose of the regulation of which it forms part',[32] the Court stressed this did not pursue the same objective as the rules on jurisdiction laid down under applicable EU legislation[33] which were instead designed to offer the weaker party stronger protection.[34]

Ilsjan principally concerned a plaintiff who was a legal person, as opposed to a natural person, hence the ruling that where a legal person pursues an economic activity, its centre of interests must reflect 'the place where its commercial reputation is most firmly established and must, therefore, be determined by reference to the place where it carries out the main part of its economic activities'.[35] Whilst observing this may coincide with the place of its registered office the Court also observed it may not always do so where the entity carried out the main part of its activities in a Member State other than where its registered office was located and where as a consequence its commercial reputation is most affected. Where this was the case, the courts of that Member State are instead best placed to assess the existence and scope of the alleged injury.

In obiter comments that are especially helpful for the arguments advanced later in this article, however, the Court articulated parallel reasoning applicable to a plaintiff who was a natural person, stating that identification of the centre of interests in this case 'generally corresponds to the Member State of his habitual residence', but that 'such a person may also have his centre of interests in a Member State in which he does not habitually reside, in so far as other factors, such as the pursuit of a professional activity, may establish the existence of a particularly close link with that State'.[36]

Similar issues have also been raised in relation to data privacy itself, where it has been suggested that the relevant test includes consideration of whether there is a 'substantial connection between the matter and the state seeking to exercise jurisdiction'.[37] While these tests represent improvements compared to the ancient data export model, this article proposes a test that is more refined than the ones proposed so far.

---

32 *eDate* (C-509/09 and C-171/10) [2011] ECR I-10269, I-10319 [38] (The Court).

33 *Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters* [2012] OJ L 351/1, ch II, ss 3–5.

34 *Folien Fischer and Fofitec v Ritrama* (Court of Justice of the European Union, C-133/11, 25 October 2012) [46].

35 *Ilsjan* (Court of Justice of the European Union, C-194/16, 17 October 2017) [41] (The Court).

36 *Ilsjan* (Court of Justice of the European Union, C-194/16, 17 October 2017) [40] (The Court), citing *eDate* (C-509/09 and C-171/10) [2011] ECR I-10269, I-10321 [49] (The Court).

37 Dan Jerker B Svantesson, 'Extraterritoriality and Targeting in EU Data Privacy Law: The Weak Spot Undermining the Regulation' (2015) 5 *International Data Privacy Law* 226, 227.

III FAILINGS OF THE DATA TRANSFER MODEL

The data transfer model is the traditional method used by data privacy laws for controlling the flow of information across national borders.[38] It is premised on the idea that a data controller has discrete items of information and it is able to control the place of that information. If a data controller decides to transfer information across a physical border, it must comply with whatever restrictions or limitations apply. The data transfer model works if the data controller is able to control the location of data, but it is less relevant in respect of modern technologies such as cloud computing, especially when files can be fragmented and spread across multiple servers.[39] In *Riley v California*[40] the US Supreme Court stated that

> [c]loud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.[41]

Information accessed from an internet enabled device such as a cellphone may be stored on the phone itself or it may be stored on a remote server or servers accessible through the cloud. The remote server(s) may be in a different country or countries. It has succinctly been stated that 'data location at any given point in time is neither a good indicator of the data user's ties to a particular location nor a fair determinant (from the perspective of the user) of the rules that ought to apply'.[42]

It has been argued that the location of storage of information is of little importance and that the focus should be on the location in which the user resides and where the content is produced.[43] According to this suggestion, 'the degree of protection accorded to particular electronic content by the United States would hinge on the nationality of the user and the location where the content originated'.[44] However, this argument on its own is not sophisticated enough to deal with the intricacies of modern data practices as well as the rationales

---

38 See *Directive 95/46* art 25, which has now been superseded by *GDPR* art 45; see also *Privacy Act 1988* (Cth) s 8.

39 *Microsoft Corp v United States*, 829 F 3d 197, 229–30 (2nd Cir, 2016).

40 573 US 373 (2014).

41 Ibid 397 (Roberts CJ). Cloud computing has been succinctly defined as a 'service whereby information, software, and shared resources are provided as a utility to electronic devices such as computers over the Internet': Joe Kong, Xiaoxi Fan and K P Chow, 'Introduction to Cloud Computing and Security Issues' in Anne Cheung and Rolf Weber (eds), *Privacy and Legal Issues in Cloud Computing* (Edward Elgar, 2015) 8, 12.

42 Jennifer Daskal, 'The Un-territoriality of Data' (2015) 125 *Yale Law Journal* 326, 374. Daskal refers to location independence, which is the idea that the efficiency of the cloud stems from its ability to allow providers to move data at any time in order to provide uninterrupted access to the user; 'the user is often blissfully ignorant of where his or her data is stored at any given moment': at 373.

43 Reema Shah, 'Law Enforcement and Data Privacy: A Forward-Looking Approach' (2015) 125 *Yale Law Journal* 543, 547–53.

44 Ibid 550.

underpinning data privacy laws globally and the arguments developed in this article are necessary to supplement its deficiencies.

The logic of these laws[45] is founded on the dangers of modern bureaucratic societies as identified in Kafka's celebrated *The Trial*.[46] These include power imbalances and vulnerabilities for individuals through a lack of transparency and accountability on the part of those processing the individual's data which, in turn, are likely to lead to mischiefs such as 'indifference, errors, abuses … [and] frustration'.[47] Accordingly, the substance of data privacy laws expressly require the balancing of the interests and rights of individuals against competing interests whenever individuals' data are processed.[48]

For example, there may be situations where the privacy interests[49] of the individual are not prejudiced in the place in which they reside, such as when a consumer in New Zealand enters data on a United States website in order to apply for a visa to enter the United States. The place in which the individual's privacy interests are prejudiced (if at all) in this example is in the United States, not in the place of nationality or the place where the content originated. On the other hand, an individual in New Zealand who accesses and enters data on a United States social networking site may have their privacy interests prejudiced in New Zealand, and therefore New Zealand laws should apply to the United States social network in respect of the data of this individual.

When such an individual enters into a contract with the overseas social networking organisation, the organisation is carrying on business in New Zealand because that is where the consumers see the information on their screens, even though the screens may be connected through the Internet to a computer in another country. If the individual consumer suffers interference with their privacy interests then the *Privacy Act 1993* (NZ) should apply. Prejudice to privacy interests in New Zealand would cover situations such as the overseas organisation using the information for sale to a health insurer. If the individual's insurance premiums are affected by the information then this is prejudice to the individual's privacy interests in New Zealand.[50] If, on the other hand, the individual happened to be an American on holiday in New Zealand temporarily, then under the logic above any prejudice to their interests when they return to the United States would be in that jurisdiction and not in New Zealand; therefore the

45 See, eg, the United States *Privacy Act of 1974*, 5 USC § 552a (1974) and the Swedish *Datalag* [Data Act] (Sweden) No 1973:289.

46 Franz Kafka, *The Trial* (Penguin, 1994).

47 Daniel J Solove, '"I've Got Nothing to Hide" and Other Misunderstandings of Privacy' (2007) 44 *San Diego Law Review* 745, 766.

48 See for instance art 6 of the *GDPR* as to the conditions for the lawfulness of processing, art 6(1)(d) where processing is necessary to protect the 'vital interests' of the data subject, art 6(1)(f) where the legitimate interests of the controller are overridden by the interests or fundamental rights and freedoms of data subjects, and art 49 derogations that refer to the interests of data subjects.

49 In this article, the term 'privacy interests' is used in the sense of data privacy interests only.

50 This would constitute a breach of principle 11 of the *Privacy Act 1993* (NZ).

Privacy Act 1993 (NZ) ought not to apply.[51] Examples are further developed in Part VII of this article.

The question that arises, against this backdrop of developments, is whether the existing data privacy paradigm, including safeguards relating to cross-border data transfers, is still fit for purpose in most respects. The argument addressed by this article is that the existing solutions need to be enhanced by additional approaches which the article articulates. Attention is first turned, however, to shortcomings in the data transfer model.

At the inception of data privacy laws cross-border data flows were 'an exceptional occurrence', whereas Kuner points out they 'are now the rule'.[52] The truth of this observation is hardly deniable. Apart from the increased outsourcing of services worldwide one only needs to consider the use of cloud services which are often located offshore. Even the smallest organisation – not to mention individuals themselves – not only avail themselves of such services but also back up their data which itself is likely to involve the use of the cloud. As a consequence, there is arguably nowadays little distinction between domestic data processing and the export of the personal data.[53] Data subjects can also experience difficulty determining the location of data processing and questions arise as to applicable law and jurisdiction: that of the data controller as opposed to the location of the data.[54] These realities have been acknowledged in the *GDPR*[55] which has extraterritorial effect, as will be discussed in Part VI of this article.

A further result has been the development of new business models that enable value to be created from this rapidly growing information infrastructure. Whilst it may be trite to describe personal data as the 'new oil' or even currency of the digital age, a Swedish study has noted that from a practical standpoint:

> Cross-border data flows have also been a driving force behind the emergence of so-called global value chains (GVCs) in which businesses' operations are fragmented across borders in order to increase efficiency, lower costs, and speed up production … Data needs to move to create value. Data sitting alone on a server is like money hidden under a mattress. It is safe and secure, but largely stagnant and underutilized.[56]

A more serious objection to data transfer restrictions also needs to be considered and that is the argument that such regulation is seriously detrimental

---

51 Unless in the unusual circumstance that there had been some prejudice to the individual's privacy interests while they were in New Zealand in which case the *Privacy Act 1993* (NZ) should apply.

52 Kuner, *Transborder Data Flows*, above n 1, 158.

53 See European Data Protection Supervisor, 'Opinion of the European Data Protection Supervisor on the Commission's Communication on "Unleashing the Potential of Cloud Computing in Europe"' (Opinion, 16 November 2012) 6.

54 Kuner, *Transborder Data Flows*, above n 1, 123. See also *Schrems* (Court of Justice of the European Union, C-362/14, 6 October 2015).

55 [2016] OJ L 119/1.

56 Kommerskollegium [National Board of Trade], 'No Transfer, No Trade – The Importance of Cross-Border Data Transfers for Companies Based in Sweden' (Report No 1, 2014) 9; see generally Kevin B Sobel-Read, 'Global Value Chains: A Framework for Analysis' (2014) 5 *Transnational Legal Theory* 364.

to the interests of individuals, corporations and society as a whole.[57] Although those subscribing to this school of thought tend to have vested interests in the conclusions reached, they nonetheless cite empirical research to support their assertions. For example, both the Chamber of Commerce Report[58] and the Swedish study[59] contain several case studies drawn from diverse sectors that hint at fundamental conceptual difficulties with regulating personal data flows.

One such instance given is the need for data integrity or the difficulties of maintaining accuracy of personal data in an era of heightened mobility.[60] This is especially evident in the credit provision and credit reporting field where a silo approach prevents credit histories from following individuals across borders.[61] This is said to be systematic of a wider problem of maintaining accurate databases in order to preserve customer relationships: 'laws that restrict the centralization of customer records increase threats to data integrity by preventing customer files from being cross-checked for errors'.[62]

A further case study relates to human resources and the management of a global workforce.[63] In the United States study one company stated: '[w]ithout cross-border transfers of personal data, [we] could not effectively pool employee data to evaluate employees against their peers outside the country of collection for ratings, promotions or assignment planning'.[64]

This is reflected in the Swedish research which hints that cross-border restrictions hinder skills-matching and the provision of equitable salary levels within corporate groups.[65] Innovation is also an issue as pointed out earlier. It is even suggested that restrictions have led companies to change their modes of delivery – not being able to move data to developers means moving the developers to the data. That is, in this case, replacing cross-border data flows with the movement of natural persons, which in turn implies other obstacles (eg, the cost of moving developers and their families, immigration procedures, and costs).[66]

The last example illustrates that the impediments referred to do not relate only to the imperatives of business efficiency. Very real human costs and potential benefits from the portability of personal information across borders are also involved. However, a consequence of enhanced information transfers across borders is that appropriate redress is needed where harms occur from the transfer. One of the benefits of extraterritorial application of data privacy laws may be the

57 Kuner gives the example of medical breakthroughs and even the detection of hitherto unknown side-effects of certain drugs from the application of data analytics to large amounts of personal data – including Big Data – collected from disparate sources across many countries, citing many reported instances: Kuner, *Transborder Data Flows*, above n 1, 4.

58 US Chamber of Commerce and Hunton & Williams, 'Business without Borders: The Importance of Cross-Border Data Transfers to Global Prosperity' (Report, 2014) 10–18.

59 Kommerskollegium, above n 56, 24–35.

60 US Chamber of Commerce and Hunton & Williams, above n 58, 7–8.

61 Ibid 8.

62 Ibid.

63 Ibid 9.

64 Ibid.

65 Kommerskollegium, above n 56, 22 [5.2.9].

66 Ibid 20 [5.2.4].

ability of an individual to access their data in another jurisdiction and to have it corrected where, say, an error has led to an inaccurate credit score.

The final case study relates to the emerging 'Industrial Internet', that is the imperative of manufacturing and energy efficiency.[67] To achieve such efficiencies companies need to be able to 'remotely collect operational data from equipment in use in locations scattered across the globe, then employ diagnostic and prognostic analyses of the data to alert customers of necessary maintenance and potential risks'.[68] Well-known examples of this phenomenon include data gathered from myriad sensors in modern vehicles that can improve road safety as well as reduce repair costs.[69]

Yet another aspect of the Industrial Internet overlaps somewhat with the first case study: '[c]loud services are commonly used in research projects to share and process scientific data, including medical data. Barriers to data transfers can incur difficulties for researchers and could delay medical advances'.[70]

The examples cited above do not, on their own, lead to the inevitable conclusion that the existing data privacy paradigm is broken. Nevertheless, despite the obvious biases of those involved in the case studies the needs highlighted by them for seamless mechanisms to exist for the transfer of personal information across borders, as well as for protections for the rights of individuals involved when transfers occur, are undeniable.

It may also be that many of the issues contained in the case studies are definitional in nature; for instance, whether they relate to personal data in the first instance and whether Big Data necessitates the creation of new rules governing its use. It will also be evident that these matters arise equally at the domestic level as well as with regard to cross-border transfers and accordingly may lead to discussion as to whether new principles are needed in the data privacy field.

Given the weaknesses that have been identified in the existing approaches to regulating cross-border data transfers,[71] an alternative framework is needed through which to protect the data privacy rights of individuals. The argument advanced in this article is that states already are asserting extraterritorial jurisdiction to protect such rights and the article accordingly seeks to validate this through creating a workable template for such an extension. Extraterritorial application generally is considered in Part VI but attention is first turned to the interface between contractual consent and mandatory domestic laws. This is

67 US Chamber of Commerce and Hunton & Williams, above n 58, 8.

68 Ibid.

69 Schonberger and Cukier give numerous illustrations of how sensor data, correlational analysis and similar methods can identify specific patters that typically occur before an actual failure takes place: Viktor Mayer-Schönberger and Kenneth Cukier, *Big Data: A Revolution that Will Transform How We Live, Work, and Think* (Houghton Mifflin Harcourt, 2013) 59.

70 Kommerskollegium, above n 56, 22 [5.2.9].

71 It has been argued that data protection regimes are incapable of regulating Web 2.0 activities, and that conventional causes of action and criminal offences are the only prospects: Paul Roth, 'Data Protection Meets Web 2.0: Two Ships Passing in the Night' (2010) 33 *University of New South Wales Law Journal* 532, 560.

because organisations often attempt to exclude the application of foreign laws through the use of contractual clauses such as forum selection and choice of law clauses. If such clauses are effective then extraterritorial application of data privacy laws is pointless.

IV CONTRACTING OUT OF LOCAL DATA PRIVACY LAWS NOT EFFECTIVE TO LIMIT THE JURISDICTION OF THE LOCAL DPA OR COURTS

Global organisations such as Amazon, Facebook and Google have sought to use forum selection and choice of law clauses to limit the ability of courts in different countries to hear claims relating to the services they provide. For example, Facebook's Terms of Service (recently updated from its former Statement of Rights and Responsibilities) includes a clause to the effect that disputes will be resolved in California under the law of the State of California (other than a dispute that 'arises out of or relates to these Terms or the Facebook Products' which now falls under the law in the consumer's own country).[72] Such clauses have been successfully challenged in the Supreme Court of Canada and the Court of Justice of the European Union ('CJEU') where they have been held ineffective to limit the jurisdiction of local courts or DPAs in the country of the consumer. A major concern is that large organisations may abuse their contracting power by the use of non-negotiable standard form contracts.[73]

In *Douez v Facebook Inc* ('*Douez*'),[74] the Supreme Court of Canada held, by a majority of four to three, that Facebook's forum selection and choice of law clause in its Statement of Rights and Responsibilities was unenforceable.[75] Forum selection and choice of law clauses are essentially a tension between freedom of contract and the public good in having local courts adjudicate claims where this is appropriate.[76] The plaintiff was claiming that Facebook was in breach of a statutory privacy tort contained in section 3(2) of the British Columbia *Privacy Act*[77] by its conduct in using her image and name for the purposes of advertising. Facebook applied for a preliminary stay of proceedings on the basis of the forum selection and choice of law clause alone. Although Facebook had argued an additional ground of *forum non conveniens* in lower courts, this ground was not argued in the Supreme Court of Canada. Karakatsanis, Wagner and Gascon JJ held that the clause should not be enforced under the common law rule in *Z I Pompey Industrie v ECU-Line N V* ('*Pompey*').[78] This rule is a two-step approach

72 Facebook, *Terms of Service* (19 April 2018) cl 4(4) <https://www.facebook.com/legal/terms>.

73 Vaughan Black and Stephen G A Pitel, 'Forum-Selection Clauses: Beyond the Contracting Parties' (2016) 12 *Journal of Private International Law* 26, 27; Kaustuv M Das, 'Forum-Selection Clauses in Consumer Clickwrap and Browsewrap Agreements and the "Reasonably Communicated" Test' (2002) 77 *Washington Law Review* 481.

74 [2017] 1 SCR 751.

75 Emir Crowne, 'Facebook's Forum Selection Clause Not "Liked" by Supreme Court of Canada' (2017) 12 *Journal of Intellectual Property Law & Practice* 831.

76 *Douez* [2017] 1 SCR 751, [1] (Karakatsanis, Wagner and Gascon JJ).

77 *Privacy Act* RSBC 1996, c 373, s 3(2).

78 [2003] 1 SCR 450.

which asks, at the first step, whether or not the forum selection clause is 'valid, clear and enforceable and that it applies to the cause of action before the court'.[79] This part of the rule involves applying the rules of contract law and any applicable defences such as unconscionability. If the clause is valid under the first step, then the second step becomes relevant. At this stage of the rule, the onus shifts to the plaintiff to show strong reasons why the clause should not be enforced. This stage of the rule adopts the 'strong cause' test from *The Eleftheria*.[80] Karakatsanis, Wagner and Gascon JJ held that the strong cause factors should be modified in the consumer context:

> When considering whether it is reasonable and just to enforce an otherwise binding forum selection clause in a consumer contract, courts should take account of all the circumstances of the particular case, including public policy considerations relating to the gross inequality of bargaining power between the parties and the nature of the rights at stake.[81]

Ms Douez met her burden to show strong cause not to enforce the forum selection clause because 'the claim involves a consumer contract of adhesion and a statutory cause of action implicating the quasi-constitutional privacy rights of British Columbians'.[82]

Abella J agreed with the decision of Karakatsanis, Wagner and Gascon JJ but gave different reasons. Her Honour held that the forum selection clause was unenforceable under the first step of the test in *Pompey*.[83] Her Honour also placed weight on the problem that arises when:

> online consumer contracts of adhesion contain terms that unduly impede the ability of consumers to vindicate their rights in domestic courts, particularly their quasi-constitutional or constitutional rights … public policy concerns outweigh those favouring enforceability of a forum selection clause.[84]

Her Honour also held that the forum selection clause was unenforceable under the doctrine of unconscionability due to inequality of bargaining power and unfairness.[85]

Abella J also raised the issue of conflict between legislative intention and a forum selection clause. Section 4 of the British Columbia *Privacy Act*[86] gives exclusive jurisdiction to the British Columbia Supreme Court to hear cases relating to the statutory privacy tort in that Act. Her Honour held that no other court within or outside British Columbia has jurisdiction in this matter and therefore there is no possibility for a forum selection clause to oust the

79 *Douez* [2017] 1 SCR 751, [28] (Karakatsanis, Wagner and Gascon JJ).
80 [1969] 1 Lloyd's Rep 237.
81 *Douez* [2017] 1 SCR 751, [38].
82 Ibid [50] (Karakatsanis, Wagner and Gascon JJ). The quasi-constitutional status of privacy is also recognised in: *Lavigne v Canada (Office of the Commissioner of Official Languages)* [2002] 2 SCR 773, [24]–[25] (Gonthier J); *Alberta (Information and Privacy Commissioner) v United Food and Commercial Workers, Local 401* [2013] 3 SCR 733, [19] (Abella and Cromwell JJ).
83 *Douez* [2017] 1 SCR 751, [96].
84 Ibid [104].
85 Ibid [112], [116].
86 RSBC 1996, c 373, s 4.

jurisdiction of the British Columbia Supreme Court.[87] The tension between contract and privacy law has been discussed in relation to forum selection clauses and the extraterritoriality provisions of the New Zealand *Privacy Act 1993*, and it has been doubted that any forum selection clause could override privacy legislation.[88]

The minority consisted of McLachlin CJ and Moldaver and Cote JJ. Their Honours held that neither step of the *Pompey* test had been satisfied and that the forum selection clause was enforceable. Their Honours held that any risks to consumers were 'best addressed through adherence to the existing system of private international law that has been carefully developed over decades to provide a measure of certainty, order and predictability'.[89] With respect, however, it is difficult to see how the system of private international law can be set in stone to the extent that it is unable to adapt to challenges presented by new social phenomena such as the rise of global corporations that do business over the Internet and the consequent vulnerability of consumers regarding their privacy rights. On the other hand, the reasons given by the majority in the Supreme Court of Canada are a logical response to the dangers presented by forum selection and choice of law clauses in the context of the growing popularity of internet transactions and the resulting need to have rules that make sense in the online context.

In *Verein für Konsumenteninformation v Amazon EU Sàrl* ('*VKI v Amazon*'),[90] the CJEU refused to uphold a choice of law clause. Amazon EU was a company established in Luxembourg. It had no registered office or establishment in Austria but it sold items to people in Austria via a website registered under a '.de' (Germany) domain name. Terms and conditions of these contracts included (prior to mid-2012) a clause stating that 'Luxembourg law shall apply'.[91] Article 6(2) of *Regulation (EC) No 593/2008 of the European Parliament and of the Council of 17 June 2008 on the Law Applicable to Contractual Obligations (Rome I)*[92] requires that a choice of law clause cannot deprive a consumer of certain mandatory protections (in this case, this meant that certain Austrian statutory provisions must apply where they could not be contracted out of). Since there were some Austrian statutory provisions that could not be contracted out of, the choice of law clause in this case was 'unfair' under article 3(1) of *Council Directive 93/13/EEC of April 1993 on Unfair Terms in Consumer Contracts*[93] because it was a not-individually-negotiated standard form clause in electronic commerce that did not tell the consumer that some

87 *Douez* [2017] 1 SCR 751, [108].
88 Alan Toy, 'Cross-Border and Extraterritorial Application of New Zealand Data Protection Laws to Online Activity' (2010) 24 *New Zealand Universities Law Review* 222, 228; Alan Toy, 'Consent to Online Privacy Policies' (2009) 15 *New Zealand Business Law Quarterly* 236, 245–6.
89 *Douez* [2017] 1 SCR 751, [159].
90 (Court of Justice of the European Union, C-191/15, 28 July 2016).
91 Ibid [30].
92 [2008] OJ L 177/6.
93 [1993] OJ L 95/29.

Austrian laws would still apply.[94] A consumer might therefore be misled into thinking that no Austrian laws applied at all.

This particular point in the case, while ostensibly based on the unfair contract terms provisions, displays the same doctrinal concern evident in *Douez* regarding the purported use of choice of law clauses to override laws in the consumer's country of residence that cannot be contracted out of. There is a fundamental conflict between mandatory aspects of some data privacy laws and the idea that these can be ousted by a simple contractual term that seeks to substitute the law of another jurisdiction.

Online contracts have been upheld, even if the terms are contained in a separate webpage, accessible by a hyperlink from the page on which the consumer is required to click assent to the terms.[95] However, there remains considerable doubt about the enforceability of online contracts that have been updated without sufficient notice being given to consumers who have repeated dealings with organisations online.[96] For example, if a consumer has agreed to the terms and conditions of a social networking website then there may be continued use of that site by the consumer. The site may have changed its terms and conditions without notice to the consumer. In these circumstances, it is unlikely that the terms will bind the consumer, even though they may contain a clause to the effect that continued use of the site will bind the consumer to the updated terms.

In a jurisdiction where there exist laws against unfair contract terms,[97] or in which the 'strong cause' test used in *Douez* may apply, or where terms of an online agreement have been updated without notice to the consumer, there would therefore seem to be significant doubt that a not-individually-negotiated standard form choice of law clause in electronic commerce would be effective. Therefore, forum selection and choice of law clauses do not present an insurmountable obstacle to the extraterritorial jurisdiction model for protecting data privacy.

V EXTRATERRITORIAL APPLICATION OF NATIONAL DATA PRIVACY LAWS

The thesis of this article is that it is the location of the business activities of the data controller/processor plus the location of the harm that should be of primary importance in the regulation of data privacy. Other considerations, such as the location of the data, should be irrelevant. Given that a state has territorial jurisdiction over harms that occur within that state,[98] can a case be made for the extraterritorial application of national data privacy laws?

---

94 Ibid [71].

95 Andrew Dickinson and Johannes Ungerer, '"Click Wrapping" Choice of Court Agreements in the Brussels I Regime' (2016) 1 *Lloyd's Maritime and Commercial Law Quarterly* 15, 18.

96 Toy, 'Cross-Border and Extraterritorial', above n 88, 230.

97 Such as New Zealand, for instance *Fair Trading Act 1986* (NZ) s 26A.

98 Andrew Keane Woods, 'Against Data Exceptionalism' (2016) 68 *Stanford Law Review* 729, 767–8.

The reason for the rise of extraterritoriality is self-evident. For instance, Kohl points to genuinely novel issues spawned by the architecture of the Internet such as the process of linking.[99] She also argues that, while the Internet has not made a qualitative difference to the conduct engaged in through it, there is nonetheless a 'vast quantitative difference'.[100] For example, the seminal decision of the High Court of Australia in *Gutnick*,[101] illustrates the greatly enhanced field of operation that can arise for defamation law as defamatory content can be downloaded throughout the world and protections that may be available to the defendant in their own jurisdiction will provide little if any shield in the jurisdiction of the plaintiff.

Svantesson puts the conundrum for states as follows:

> extraterritorial jurisdictional claims are reasonable because if states do not extend their data protection to the conduct of foreign parties, they are not providing effective protection for their citizens. At the same time, extraterritorial jurisdictional claims may be argued to be unreasonable because it is not possible for those active on the Internet to adjust their conduct to all the laws of all the countries in the world with which they come into contact.[102]

Traditionally there has been a presumption against extraterritorial application of statutes and it has been stated that '[w]hen a statute gives no clear indication of an extraterritorial application, it has none'.[103] However, especially in relation to online activity, the presumption against extraterritorial application is abating.[104] *GDPR* has now superseded the EU's *Directive 95/46* which formerly specified that it was only to be applied in national provisions when the 'processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State'[105] or where

> the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.[106]

It will be seen that *GDPR* goes much further than *Directive 95/46* in its statement of extraterritorial effect. This Part will discuss recent cases that have taken an expansive approach to extraterritorial jurisdiction. In addition, national data privacy laws, as they become updated, are gaining greater extraterritorial powers. It has been noticed that there is a 'trend towards local data protection regulations attempting to capture any activity that is targeted at local residents, regardless of the actual location of the business'.[107]

---

99 Uta Kohl, *Jurisdiction and the Internet: Regulatory Competence over Online Activity* (Cambridge University Press, 2007) 36.

100 Ibid 39.

101 (2002) 210 CLR 575.

102 Svantesson, *Extraterritoriality in Data Privacy Law*, above n 12, 21.

103 *Morrison v National Australia Bank Ltd*, 561 US 247, 255 (2010) (Scalia J).

104 Toy, 'Cross-border and Extraterritorial', above n 88, 225.

105 *Directive 95/46* art 4(1)(a).

106 *Directive 95/46* art 4(1)(c).

107 United Nations Conference on Trade and Development, 'Data Protection Regulations and International Data Flows: Implications for Trade and Development' (Report, United Nations, 2016) 20 <http://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=1468>.

In *VKI v Amazon*,[108] the CJEU held that the former *Directive 95/46* applied the local laws in a Member State of the EU where processing of personal data is performed in the context of an undertaking engaged in electronic commerce, provided that the undertaking directs its activities to the Member State in which the consumer resides and there is a sufficient establishment of the undertaking in that place (which may require less than having a branch or subsidiary in the consumer's locality but would require more than simply having a website accessible there).[109] The important factors in making this determination include the 'degree of stability of the arrangements and the effective exercise of activities in the Member State in question'.[110] *Weltimmo s r o v Nemzeti Adatvédelmi és Információszabadság Hatóság* ('*Weltimmo*')[111] holds that the concept of 'establishment' within the former *Directive 95/46* 'extends to any real and effective activity – even a minimal one – exercised through stable arrangements'.[112] This test requires that

> both the degree of stability of the arrangements and the effective exercise of activities in [the Member State] must be interpreted in the light of the specific nature of the economic activities and the provision of services concerned. This is particularly true for undertakings offering services exclusively over the Internet.[113]

In *Weltimmo*, a company registered in Slovakia ran property dealing websites relating to properties in Hungary which were written in Hungarian. Weltimmo had one representative in Hungary who was listed in the Slovak companies register with an address in Hungary. This representative was a contact point for complainants in Hungary. Weltimmo had opened a bank account in Hungary and had a letter box in Hungary. It was held that this was enough to constitute a real and effective activity in Hungary and Weltimmo therefore had an 'establishment' in Hungary.[114]

Although *Directive 95/46* has now been superseded by the *GDPR*, the concept of establishment is still relevant as the *GDPR* preserves this approach through limiting its scope to 'the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union'.[115] However, the extraterritorial reach of the *GDPR* is potentially much stronger than under *Directive 95/46* and it marks a radical point of departure through extending the scope of the regulation:

> [T]o the processing of personal data of data subjects who are in the Union by a controller not established in the Union, where the processing activities are related to:
>
> (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

108 *VKI v Amazon* (Court of Justice of the European Union, C-191/15, 28 July 2016).
109 Ibid [76], [81].
110 Ibid [77].
111 (Court of Justice of the European Union, C-230/14, 1 October 2015).
112 Ibid [31].
113 Ibid [29].
114 Ibid [32]–[33].
115 *GDPR* art 3(1).

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.[116]

While the concept of 'establishment' is still clearly relevant, a far broader range of conduct will be subject to the *GDPR* when it comes into force. This amounts to a significant expansion of the jurisdiction of the European data protection regime. It may be argued that the extraterritorial application of the *GDPR* is too broad. Svantesson criticises the provision as:

> likely to bring all providers of Internet services such as websites, social networking services and app providers under the scope of the EU Regulation as soon as they interact with data subjects residing in the European Union … the new approach … more clearly emphasizes the significant extraterritorial dimension of the data privacy law … Article 3 of the proposed Regulation has a worrying potential for absurdity.[117]

Such an approach has already been adopted by Australia where the Australian Privacy Principles extend to 'an act done, or practice engaged in, outside Australia and the external Territories by an organisation, or small business operator, that has an Australian link'.[118] This would include overseas companies that carry on business in Australia or an external Territory and collect or hold personal information in Australia or an external Territory, either before or at the time of the act or practice.[119]

The term 'carries on business in Australia' is not defined in legislation[120] although some guidance as to its meaning may be available from areas of the law other than data privacy law in that country.[121] The mere existence of a website that may be accessed in Australia is not sufficient,[122] but other conduct – such as being the registered proprietor of trade marks in Australia,[123] the collection of personal information from individuals physically in Australia,[124] operating a website offering goods or services to countries that include Australia or where Australia is one of the countries on the drop down menu appearing on the entity's website[125] – can amount to carrying on business in Australia.

Thus, overseas companies offering goods or services in Australia would need to comply with Australia's legal requirements prior to collecting any personal information, a position not dissimilar to that under the *GDPR*. On the other hand, it can be observed that the Australian business connection test described above intersects with both the concept of establishment within the former *Directive 95/46* and the somewhat wider test contained under the *GDPR*. It remains to be seen if the interpretation given to the concept of 'offering goods and services' under *GDPR* is more expansive than in Australia. Svantesson has suggested the

116 *GDPR* arts 3(2)(a)–(b).
117 Svantesson, *Extraterritoriality in Data Privacy Law*, above n 12, 107.
118 *Privacy Act 1988* (Cth) s 5B(1A).
119 *Privacy Act 1988* (Cth) s 5B(3).
120 *Privacy Act 1988* (Cth) s 5B(3)(b).
121 Office of the Australian Information Commissioner, 'Australian Privacy Principles Guidelines: *Privacy Act 1988*' (Guidelines, February 2014) 5–6 [B.13]–[B.15].
122 *Gebo Investments (Labuan) Ltd v Signatory Investments Pty Ltd* (2005) 190 FLR 209, 220–1 (Barrett J).
123 *Australian Wool Innovation Ltd v Newkirk [No 3]* [2005] FCA 1308, [34] (Hely J).
124 Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (Cth) 218.
125 Office of the Australian Information Commissioner, above n 121, 5 [B.14].

GDPR formulation adopts what he calls a 'targeting' approach drawn from consumer law based on the subjective intention of the company involved.[126] He sees this as unwelcome as it potentially catches the practices of overseas organisations even where no customers in the EU are procured.[127] By contrast, the approach advocated in this article, whilst sharing Svantesson's concerns, advances a means through which they may be addressed.

It is the second limb, that of paragraph (b), 'monitoring the behaviour of' data subjects in the Union, which introduces a potentially limitless extension of extraterritoriality. Much will depend on the interpretation of this term. It does not seem unnatural to suggest that monitoring the behaviour of data subjects could extend to virtually any activity that is capable of identifying the subjects. In theory, few internet activities would be immune from this phrase. The application of the concept to 'data subjects', however, presumably refers to them in an individual capacity as many modern marketing practices involve surveillance of patterns of behaviour by groups of individuals exhibiting certain characteristics.

It is also important to note that, for application of the former *Directive 95/46*, processing of personal data had to be performed in the context of an undertaking engaged in electronic commerce but did not need to be performed by the undertaking itself. Merely processing in the context of the undertaking was sufficient.[128] This point indicates that the actual location of the data was unimportant, and may of course be difficult or impossible to ascertain with the tools at the disposal of any of the parties involved in the dispute.

As has already been demonstrated, the location of the processor is of little relevance, provided the processor has an establishment within the territory of the consumer's country. In *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* ('*Google Spain and Google*')[129] Google Inc processed the data, but this processing was not carried out by its local subsidiary, Google Spain (which existed solely for the purpose of supporting Google's advertising activity).

The CJEU held that the establishment itself did not have to carry out the processing and that the requirement that the processing was carried out 'in the context of the activities' of the establishment was satisfied in this case.[130] The purpose of Google Spain was to secure advertising revenues for Google within Spain, and this activity served to make the data processing activities of Google Inc profitable. This case demonstrates that the location of the processing or of the data processor itself is almost irrelevant to the effective exercise of data privacy rights of consumers.

---

126 Svantesson, 'Extraterritoriality and Targeting in EU Data Privacy Law', above n 36, 231.

127 Ibid 232.

128 *VKI v Amazon* (Court of Justice of the European Union, C-191/15, 28 July 2016) [78]; *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* (Court of Justice of the European Union, C-131/12, 13 May 2014) [52] ('*Google Spain and Google*'); *Weltimmo* (Court of Justice of the European Union, C-230/14, 1 October 2015) [35].

129 (Court of Justice of the European Union, C-131/12, 13 May 2014).

130 Ibid [55] (The Court).

The key point to note, however, is that under the *GDPR*, even if Google Spain had not existed, the activities of Google Inc in processing the data may well also have amounted to the monitoring of their behaviour under paragraph (b). This is because the search engine's automated processes had identified the complainant from information about him contained in a recently digitised repository. It is in response to this extension that the present article argues for the adoption of an additional requirement that the privacy interests of the individual must be prejudiced in the jurisdiction seeking to exert its law extraterritorially. Without such a filter the net cast by *GDPR* may be too wide.

In *Microsoft Corp v United States*[131] (which was a warrant case, not a data privacy case), Microsoft held certain email data on servers in Ireland. A warrant issued under the *Stored Communications Act* (US) ('*SCA*')[132] directed Microsoft to send the email data from Ireland to the US and then produce it pursuant to the warrant. The argument for the United States government in the case was that the production of data by a United States organisation is not extraterritorial because that organisation is able to electronically access the data even if it is stored in other countries.[133] The argument made for the United States government was a consequence of its concession that the *SCA* does not have extraterritorial effect.[134] The argument that extraterritoriality was not involved in the case was rightly rejected by the United States Court of Appeals for the Second Circuit, which held that 'to enforce the Warrant, insofar as it directs Microsoft to seize the contents of its customer's communications stored in Ireland, constitutes an unlawful extraterritorial application of the Act'.[135] The opposite conclusion was reached in *In re Search Warrant No 16-960-M-01 to Google* in which it was decided that there was neither a search not a seizure of the targets' data in a foreign country.[136] Although the decisions are now moot due to passage of the *Clarifying Lawful Overseas Use of Data Act* (US) ('*CLOUD Act*')[137] in 2018, this statute strongly supports our argument in this article. The *CLOUD Act* implicitly recognises the concept of where individuals' and governments' interests are affected most

131 829 F 3d 197 (2nd Cir, 2016); see also the denial of rehearing en banc: *Microsoft Corp v United States*, 855 F 3d 53 (2nd Cir, 2017).

132 *Electronic Communications Privacy Act of 1986* 18 USC § 2510 contains Title II, which is referred to as the *Stored Communications Act* 18 USC §§ 2701–13.

133 *Microsoft Corp v United States*, 829 F 3d 197, 229 (2nd Cir, 2016) (Lynch J).

134 Ibid 210 (Carney J).

135 Ibid 221 (Carney J). In the denial of rehearing en banc, the dissent relied on an argument that the location of the data or of the processing is irrelevant: 'Localizing the data in Ireland is not marginally more useful than thinking of Santa Claus as a denizen of the North Pole … reifying the notional: Where in the world is a Bitcoin? Where in my DVR are the images and voices? Where are the snows of yesteryear?': *Microsoft Corp v United States*, 855 F 3d 53, 62 (Jacobs J) (2nd Cir, 2017). While this argument has an alluring simplicity, it is based on the practical and legal restrictions in the case against recognition of extraterritorial application of the warrant provisions of the *SCA* and does not represent a principled basis on which to understand the complex issues of extraterritoriality in the context of online activity. The Supreme Court of the United States granted leave to appeal: *United States v Microsoft Corporation*, 199 L Ed 2d 261 (2017).

136 *In re Search Warrant No 16-960-M-01 to Google*, 232 F Supp 3d 708, 719 (ED Pa, 2017) (Rueter J).

137 Pub L No 115-141, div 5, 132 Stat 348, 1213 (2018).

strongly,[138] as well as acknowledging that the location of data is irrelevant.[139] It may be suggested therefore that the resolution of this issue in relation to warrants under United States law at least has been resolved by the same principle that we propose in our argument.

It was acknowledged in *Microsoft Corp v United States* that '[t]he tricky part, in a world of transnational transactions taking place in multiple jurisdictions at once, is deciding whether a proposed application of a statute is domestic or extraterritorial'.[140] The argument in this article is that data privacy laws do have extraterritorial effect where an organisation in a country (Country A) controls the data of a consumer who was in another country (Country B) when the data was collected provided the organisation has a business link with (or conducts activities in) Country B and the privacy interests of the consumer are prejudiced in Country B as a result of action or inaction by the data controller. In these circumstances, we argue that data privacy laws in force in Country B should have application and that this application is not merely a domestic application of local laws. To classify any application of data privacy laws as domestic simply because the consumer is located in Country B and the conduct affects them there is overly simplistic and does not take account of the business link test which is an essential part of our analysis. Provided that the data controller is in Country A (regardless of whether the data is in Country A) then data privacy laws may have extraterritorial effect.

Furthermore, one of the derogations under the former *Directive 95/46* and under the *GDPR* – standard contractual clauses – in essence, contains characteristics of the extraterritorial approach as it seeks to impose a EU data privacy standard to conduct that is likely to occur, in respect of the personal data, outside the EU. For example, a contract between an exporter and an importer will impose ongoing duties on the exporter to monitor compliance, by the latter with its obligations.

Nonetheless, several limitations exist as to the practicality of such derogations. As far as the data subject is concerned, enforceability hinges largely on the existence, within the country of destination, of third-party beneficiary rights that go beyond the confines of contractual privity. Although this may exist in countries within the EU,[141] the same cannot be said of the global environment in which business is now conducted.

Under the further derogation of Binding Corporate Rules ('BCRs'), on the other hand, enforcement of data privacy rights can only be ensured indirectly,

---

138 Section 3 contains a comity analysis, which refers specifically to the 'nature and extent of the subscriber or customer's connection to the United States … [and] the nature and extent of the provider's ties to and presence in the United States'. The interests of the United States and the qualifying foreign government are likewise relevant.

139 The *CLOUD Act* section 3 also states that the obligation to comply with the Act applies 'regardless of whether such communication, record, or other information is located within or outside of the United States'.

140 *Microsoft Corp v United States*, 829 F 3d 197, 226 (2nd Cir, 2016) (Lynch J).

141 Christopher Kuner, *European Data Protection Law: Corporate Compliance and Regulation* (Oxford University Press, 2nd ed, 2007) 226–7 [4.132].

through enforcement in the country of export. For example, *GDPR* contains detailed provisions regarding BCRs, in particular:

> the acceptance by the controller or processor established on the territory of a Member State of liability for any breaches of the binding corporate rules by any member concerned not established in the Union.[142]

Such liability may be described as being through accountability – the liability of principals for the conduct of agents and others being an accepted notion in most legal systems – but must be distinguished from extraterritorial application of domestic law. The three possible approaches to regulation where cross-border data transfers of personal data are involved are therefore export prohibitions or restrictions, accountability as an intermediate option, and extraterritoriality.

VI THE EFFICACY OF THE EXTRATERRITORIAL JURISDICTION MODEL TO ENFORCE DATA PRIVACY RIGHTS

Even if a state has prescriptive and adjudicative jurisdiction over internet activity, if it is unable to enforce its judgments then the law is toothless. If an organisation has personnel or physical assets or funds within a country then it has a strong incentive to comply with local laws.[143] However, does an organisation that has no presence in a country other than a locally accessible website have any incentive to comply with local data privacy laws?

There have now been orders that purport to affect an organisation's conduct on a global scale, the equivalent of trying to 'kill a mosquito with a nuclear bomb'.[144] However, the nuclear bomb metaphor does not accurately capture the effect of extraterritorial jurisdiction. From a practical standpoint, Kohl observes that perception of a foreign law's legitimacy is more important than its strict enforceability,[145] a view also taken by Svantesson.[146] He has in a similar vein referred to the 'bark' jurisdiction of privacy authorities, as opposed to their 'bite' jurisdiction.[147]

The ability to 'name and shame' non-compliant organisations is one such avenue.[148] The ability of privacy authorities to investigate privacy breaches across borders is another and has been upheld in a Canadian case where the Privacy Commissioner's refusal to investigate a complaint against a United States-based corporation was subject to successful judicial review.[149] Anecdotal evidence also

142 *GDPR* art 47(2)(f).
143 Woods, above n 98, 770.
144 Dan Jerker B Svantesson, 'Jurisdiction in 3D – "Scope of (Remedial) Jurisdiction" as a Third Dimension of Jurisdiction' (2016) 12 *Journal of Private International Law* 60, 63.
145 Kohl, above n 99, 208–9.
146 Svantesson, 'Extraterritoriality and Targeting in EU Data Privacy Law', above n 34, 233.
147 Dan Jerker B Svantesson, 'The Extraterritoriality of EU Data Privacy Law – Its Theoretical and its Practical Effect on US Businesses' (2014) 50 *Stanford Journal of International Law* 53, 58–60.
148 See for instance *個人資料保護法* [Personal Data Protection Act] (Macau) 8/2005 arts 43–4; *Personal Data (Privacy) Ordinance* (Hong Kong) cap 486, s 48(2), (4) (power to issue reports in the public interest); cf New Zealand where the Privacy Commissioner may make adverse comment only after the person concerned has been given an opportunity to be heard: *Privacy Act 1993* (NZ) s 120.
149 *Lawson v Accusearch Inc dba Abika.com* [2007] 4 FCR 314.

suggests that 'bark' jurisdiction is effectual with companies routinely paying fines rather than risking adverse publicity.[150]

The ability of regulators to obtain extra-territorial evidence, currently another weakness, is likewise not an insurmountable hurdle. The *US SAFE WEB Act of 2006*,[151] for example, not only broadens reciprocal information sharing but confirms the Federal Trade Commission's remedial authority in cross-border cases. It sanctions a range of solutions, including participation in foreign litigation and staff exchanges with overseas counterparts that could be a model for other cross-jurisdictional co-operation. In an increasingly globalised environment it may be impossible for domestic privacy authorities to be effective without such co-operation from their peers.

While the foregoing may be areas for future investigation, the present article does not focus on the enforcement aspect of jurisdiction, instead drawing on the reasoning of *Ilsjan* to argue for a rule of prescriptive and adjudicative jurisdiction that allows for the extraterritorial application of data privacy laws in limited circumstances. In this context its thesis is that extraterritorial jurisdiction may be exerted over only those organisations that satisfy the tests proposed (first, that the organisation does business[152] in the country and second, the individual citizen's privacy interests are also prejudiced in that country). This is a selective test under which the article argues it is legitimate for a country to control the conduct in question.

As has been seen, the business connection test has already been adopted in several jurisdictions. The concept of prejudice to an individual's rights, on the other hand, is less well understood but nonetheless found in the fabric of most data privacy laws globally.[153] It is, for instance, found throughout the *GDPR*. Article 6(1)(f) for example provides for the legitimate interests of the controller except where these are overridden by the interests or fundamental rights and freedoms of the data subject.[154] Similarly, article 21(1) provides the right to object again being founded on the balance between compelling legal grounds for the processing on the one hand and the interests or fundamental rights and freedoms of data subjects on the other, whilst articles 22(2)–(3) allow profiling provided there are suitable measures to safeguard the data subject's legitimate interests.

Kuner has stated that

> [t]he definition of "legitimate interest" varies depending on national law, but generally includes basic information rights such as "the interest of everyone in

150 Interview with Ken Chongwei Yang, Deputy Coordinator, Office for Personal Data Protection, Macao Special Administrative Region (Macao Special Administrative Region), 14 July 2014.

151 15 USC §§ 41 ff (2006).

152 Business being loosely defined to encompass 'activity' and not business in the strict economic sense.

153 See, eg, *Directive 95/46* art 7(d) referring to the 'vital interests' of data subjects and *Privacy Act 1993* (NZ) s 6, principle 2(2)(c) stating 'non-compliance would not prejudice the interests of the individual concerned'.

154 The nature of the principles as being fundamental principles is discussed in Alan Toy, 'Different Planets or Parallel Universes: Old and New Paradigms for Information Privacy' (2013) 25 *New Zealand Universities Law Review* 938, 946–8.

> 'significant decisions' affecting them being taken on factual, accurate and relevant information, or the related interest in being able to challenge decisions reached on the basis of erroneous or irrelevant information".[155]

It may be observed these essentially relate to the underlying rationale and logic of data privacy laws that govern how personal information is collected and used.[156]

The efficacy of the two-tier test advocated in this article may be tested by its application to some hypothetical but realistic scenarios that are likely to occur in concrete instances. Two were explored in Part III above: one of an individual in New Zealand interacting with an official United States agency in order to apply for a visa, and another of an individual accessing a United States social networking site. In the first, it is unlikely either limb would be satisfied meaning any recourse would have to be in the United States.[157] In the second, however, assuming the individual's interests are prejudiced in New Zealand – for instance, the social networking site experienced a major data breach resulting in harm to the individual in New Zealand – it is arguable the defendant ought to be held to account in New Zealand for contravening its privacy laws.[158]

The global proliferation of laws requiring notification to individuals and authorities when privacy breaches occur is worthy of comment in this context. As with other areas of data privacy this legislative trend has arisen despite the difficulty of quantifying the nature of harms that are sought to be addressed by it. Where data breaches occur, for instance, individuals who do suffer harm may be unwilling to publicise its extent or even occurrence. Consider for example the 2015 hack of the adult dating site Ashley Madison which undoubtedly led to numerous instances of blackmail.[159] Rights-based rationales for data breach notification tend to be based on the proposition that the individuals to whom the data pertains are in the best position to know what risk the breach poses to them and to be able to take steps to mitigate against these.[160]

---

155 Kuner, *European Data Protection Law*, above n 141, 77, quoting Douwe Korff, 'Study on the Protection of the Rights and Interests of Legal Persons with Regard to the Processing of Personal Data Relating to Such Persons' (Final Report ETD/97/B5-9500/78, Commission of the European Communities, October 1998) 42.

156 David Lindsay has pointed to the lack of clarity underlying such laws: David Lindsay, 'An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law' (2005) 29 *Melbourne University Law Review* 131, 133; but see the more sanguine view taken by Bygrave who points to privacy as a core value and fundamental interests including related interests such as 'personality' and 'personal integrity': Bygrave, above n 4, 118.

157 See, eg, *Privacy Act of 1974*, 5 USC § 552a (1974).

158 Currently the *Privacy Act 1993* (NZ) but law reform proposals including mandatory reporting of data breaches are currently awaiting implementation: Law Commission *Review of the Privacy Act 1993: Review of the Law of Privacy Stage 4* (NZLC R123, 2011).

159 Rachel Hosie, 'Ashley Madison Hacking: What Happened when Married Man was Exposed', *The Independent* (online), 16 January 2017 <https://www.independent.co.uk/life-style/love-sex/ashley-madison-hacking-accounts-married-man-exposes-cheating-website-infidelity-rick-thomas-a7529356.html>.

160 See Sara M Smythe 'Does Australia Really Need Mandatory Data Breach Notification Laws – And If So, What Kind?' (2013) 22 *Journal of Law, Information and Science* 159, 161–2.

Wider societal benefits, in the case of breach notification, is likewise hard to calculate for similar reasons. Identify theft is a well-accepted phenomenon[161] but other less calculable benefits may be a reduction in insurance premiums for companies as well as individuals who may otherwise experience identity theft, as well as the impetus notification laws provide for firms to improve their data management practices thereby resulting in a gain for both individuals and economic efficiency.

Consider, furthermore, an extension of the scenarios discussed above where an individual wishing to visit the United States uses the services of a consultancy based there which offers its services worldwide. Assume for present purposes the individual wishes to pursue a professional activity in the United States, perhaps a series of concerts if they happen to be an artist, or a series of lectures if they happen to be an academic or speaker. Assume also that due to the careless actions of the firm in transmitting accurate information to the relevant authorities the visa is either denied or delayed, resulting in reputational and financial loss to the individual concerned.

In this scenario, application of the business connection link – although tenuous – may well be argued. The difficulties of the targeting approach, identified by Svantesson, such as whether subjective or objective intention are relevant might well be traversed. It is unlikely, though, that the privacy interests of the individual in this instance may be said to have been prejudiced in New Zealand and therefore any attempt to bring the defendant before a tribunal in New Zealand is likely to be struck out. This does not, of course, preclude the individual proceeding against the defendant in a United States forum, perhaps for unfair or deceptive acts or practices, in or affecting commerce under its own legislation.[162] The scenario illustrates the utility of the two-tier approach and helps to circumvent the difficulties and absurdities identified by Svantesson and others.

The concept of where an individual's interests are prejudiced has its counterpart in other areas of law. In New Zealand, the statutory requirement that a company registered there must have one or more directors who 'live in New Zealand'[163] has occasioned judicial scrutiny. In *Re John Malcolm Carr*[164] a director spent less than half a calendar year in New Zealand but had residences in as well as professional and personal ties (such as a spouse, membership in social clubs and his primary care physician) in New Zealand. In finding that physical presence in New Zealand was not the principal determinant in applying the

161 Sasha Romanosky, Rahul Telang and Alessandro Acquisti, 'Do Data Breach Disclosure Laws Reduce Identity Theft?' (2011) 30 *Journal of Policy Analysis and Management* 256, 260.

162 *Federal Trade Commission Act of 1914*, 15 USC § 45 (1914); see generally Gehan Gunasekara and Jingyi Xiong, 'Lost in Translation? Privacy and Unfair or Deceptive Acts or Practices in Commerce in the United States' (2016) 22 *New Zealand Business Law Quarterly* 162.

163 *Companies Act 1993* (NZ) s 10(d)(i).

164 [2016] NZHC 1536.

statutory requirement the Court found that this was rather the capacity to enforce obligations against directors and to hold them to account.[165]

If a similar logic is applied where data privacy is concerned, a state's interests are founded on their need to protect the fundamental rights and freedoms of data subjects. A purposive approach should thus focus on the imperatives of data privacy law such as the ability of an individual to access information concerning them and to correct it, to ensure the data is secure and to prevent its misuse and improper disclosure.[166] There must, however, be a causative link between contravention of such norms and the prejudice suffered by the individual.

Although the argument put forward in this article draws on the reasoning in *Ilsjan*, it must be recognised that that case was based on the specific EU rules of jurisdiction discussed above. Nonetheless this article maintains such an approach ought to be adopted worldwide and not be confined to the ambit of the EU. It is an approach, furthermore, that may be taken by legislation in any country that wishes to adopt it and does not need to be preceded by any international treaties, conventions or similar instruments. It is unlikely that an international treaty 'forged out of pixie dust' will be achievable in relation to application of data privacy laws.[167] It is unnecessary for all countries or any particular number of countries to adopt the test proposed by this article in order for it to be effective for any country that does adopt it because the test does not require support in any country other than the one introducing it.

Many legislative codes governing data privacy, for example, require the plaintiff to have suffered a measurable harm as a prerequisite to obtaining judicial and other redress.[168] These may include material loss, adverse effects on rights, benefits, privileges, obligations and interests, significant humiliation, loss of dignity or injury to feelings or humiliation. Any state wishing to extend its data privacy requirements extraterritorially to an organisation with a business link to it must also demonstrate that the privacy interests of the individuals concerned are prejudiced or likely to be prejudiced as regards these harms. Where individuals pursue remedies in concrete instances affecting them this will be self-evident. However, this may also be the case where a regulator seeks to address systemic privacy harms such as occurred in *Schrems*.[169] In the case of the latter category the focus will be on the risks posed to the privacy interests of individuals rather than harms per se.

Adoption of such an approach would assuage many of the concerns regarding extraterritoriality canvassed above. It is important to stress that whatever the

165 Ibid [15] (France J).

166 Organisation for Economic Co-operation and Development, above n 17, 13–17.

167 Woods, above n 98, 781. Convention 108 of the Council of Europe is the closest thing to an international data privacy treaty, which has a small number of parties from outside Europe, in addition to its European parties: *Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data*, opened for signature 28 January 1981, CETS No 108 (entered into force 1 October 1985). This convention has now been modernised: Council of Europe, *Modernisation of Convention 108* (2018) <https://www.coe.int/en/web/data-protection/convention108/modernised>.

168 See, eg, *Privacy Act 1988* (Cth) ss 25–25A; *Privacy Act 1993* (NZ) s 66.

169 (Court of Justice of the European Union, C-362/14, 6 October 2015).

merits of the argument that states ought to be able to assert their 'informational sovereignty'[170] in the domestic context, this concept cannot justify states exerting extraterritorial jurisdiction – even where the defendant has a business link with the state – when they are unable to demonstrate how an individual's privacy interests have been prejudiced in the state. In other words, 'data sovereignty' cannot be applied in an abstract manner. Where prejudice can be shown, however, the extraterritorial application of data privacy law may be seen to be legitimate.

The adoption of such an approach would mean that even the expansive approach of the *GDPR* would be subject to reasonable constraint. Take, for instance, *Google Spain and Google*. Should the as yet untested 'monitoring' criterion have been engaged in this case, the plaintiff would have had to demonstrate prejudice to their interests in Spain. Of course, the nub of his complaint was precisely this, due to reputational and other interests alleged to have been affected. In other less concrete instances of monitoring, however, say where behavioural monitoring has taken place, the state ought not to be able to assert extraterritorial jurisdiction unless it can demonstrate specific harm to the privacy interests of individuals.

One final issue concerns the possibility of double jeopardy. This arises in the criminal law where a crime may have multiple locations and the solution to the problem may also be relevant to data privacy law. Where a person has served a sentence for a crime in one jurisdiction then the doctrine of autrefois convict and autrefois acquit may prevent that person being convicted a second time in another jurisdiction.[171] In the House of Lords in *Treacy v Director of Public Prosecutions*, Lord Diplock stated that:

> the rules of international comity … do not call for more than that each sovereign state should refrain from punishing persons for their conduct within the territory of another sovereign state, where that conduct has had no harmful consequences within the territory of the state which imposes the punishment.[172]

This statement dovetails neatly with the test we have proposed because our test requires prejudice to the interests of the individual within the jurisdiction. Once that is found then there is no need to ascertain the location of the conduct that harms the privacy interests of the individual (provided there is a link between the business or activities of the data controller and the jurisdiction within which the individual is located).

VII CONCLUSION

As data privacy laws mature, they have the potential to become more capable of protecting the fundamental rights that they stand for. This article has argued that there are currently two main approaches to the regulation of cross-border transfers of data: the data transfer model and the accountability model. But these

170 See Bygrave, above n 4, 125.

171 *Treacy v Director of Public Prosecutions* [1971] AC 537, 562 (Lord Diplock).

172 Ibid 564 (Lord Diplock).

two models are no longer enough on their own to protect data privacy. The extraterritorial application of data protection laws should gain greater capacity to support the aforementioned models through legislative amendment which clarifies the application of data protection laws to certain actors who may be in a foreign country. The extraterritorial model should be limited by the test that we propose in this article to avoid overly broad application to overseas organisations.

Consumers have been at risk from the activities of global organisations that conduct business online because forum selection and choice of law clauses have formerly presented a daunting obstacle to the hapless consumer who likely has little ability to enforce their rights by bringing a case[173] in a foreign country in order to protect their data privacy. Recent cases have demonstrated that the power of such clauses is beginning to diminish and this raises the possibility that the extraterritorial model may be of greater assistance in future to protect data privacy rights in the context of transnational transactions.

The data transfer model and the accountability model are no longer enough on their own to represent effective protection in the face of cloud computing and increased surveillance of citizens. This article has argued that the extraterritorial model could emerge to assist them through legislative amendment in any country that wishes to promote this model. Refinements are necessary to enable this ascension to occur, and this article has suggested that where an organisation has a business link with the place of the consumer and the consumer's privacy interests would be prejudiced in that place then the data privacy laws of that place should apply extraterritorially if necessary to control the conduct of the data controller/processor. This metamorphosis is imperative and may be inevitable.

173 In countries that have no avenue for individuals to bring such a case, there may be a DPA that can take action, but this kind of regulation may also suffer from the difficulties of cross-border enforcement.