A "layered approach" to the extraterritoriality of data privacy laws

Dan Jerker B. Svantesson*

Abstract

- The extraterritoriality of data privacy laws is emerging as a major issue.
- Current approaches to delineating the extraterritorial scope of data privacy laws are flawed, and no improvements can be expected as long as we cling on to the binary tests typically used in international law.
- The multifaceted nature of data privacy law necessitates a departure from one size fits all style delineations of extraterritoriality in favour of a more nuanced and sophisticated approach, and this article puts forward one such option in the form of a 'layered approach'.

Introduction

The extraterritorial application of a country's data privacy laws may severely impact the free speech and financial interests of other countries and their citizens. Yet, around the world, data privacy laws with extraterritorial scope are being introduced or reformed without much discussion, debate, or visible opposition. Indeed, we are currently witnessing an unprecedented level of data privacy laws being enacted (eg Singapore and Malaysia) or revised (eg Australia and the European Union) around the world.

Most importantly, the European Union (EU) is in the process of modernizing its data privacy law by replacing its Data Protection Directive 1995[1] with a new data protection Regulation.[2] Interestingly, that Regulation, with its potential for penalties of up to 2 per cent of an offending enterprise's annual worldwide turnover, looks likely to apply also to any non-EU enterprise that processes data about persons residing in the EU under certain circumstances. This means that the EU law, with its potential for heavy fines and wide extraterritorial scope, is likely to directly affect businesses around the world.

As noted elsewhere,[3] in essence, the conundrum we are faced with can be expressed 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, wide extraterritorial jurisdictional claims are arguably 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. In other words, a widespread extraterritorial application of state law may well end up making it impossible for businesses to engage in cross-border trade.

On some occasions, articles in this journal have dealt with extraterritoriality in some detail. Most specifically, in two articles published during the journal's first year, Moerel addressed the extraterritoriality of EU data privacy law.[4] Further, the editorial of issue 3(3) of this journal sought to bring attention to this important

* Professor and Co-Director, Centre for Commercial Law, Faculty of Law, Bond University (Australia); researcher, Swedish Law & Informatics Research Institute, Stockholm University (Sweden). Professor Svantesson is the recipient of an Australian Research Council Future Fellowship (project number FT120100583). The views expressed herein are those of the author and are not necessarily those of the Australian Research Council. The author wishes to thank the anonymous reviewer(s) who provided many insightful and useful comments on the text.

1 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 OJ (L 281).

2 *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 (25 Jan. 2012).

3 Christopher Kuner, Fred H Cate, Christopher Millard, and Dan Svantesson, 'Editorial: The extraterritoriality of data privacy laws—an explosive issue yet to detonate' (2013) 3(3) *International Data Privacy Law* 147, at 147–8.

4 Lokke Moerel, 'The long arm of EU data protection law: Does the Data Protection Directive apply to processing of personal data of EU citizens by websites worldwide?' (2011) 1(1) *International Data Privacy Law* 23, and Lokke Moerel, 'Back to basics: when does EU data protection law apply?' (2011) 1 (2) *International Data Privacy Law* 92.

© The Author 2013. Published by Oxford University Press. All rights reserved. For Permissions, please email: journals.permissions@oup.com

www.manaraa.com

topic.[5] In addition, some important recent works, such as a monograph titled *Transborder Data Flows and Data Privacy Law* by Kuner—editor-in-chief of *International Data Privacy Law*—engage with the question of the extraterritoriality of data privacy laws.[6]

Yet, there can be no suggestion that a final, optimal, and agreeable to all solution has been found. In this article, I outline a proposal for an alternative—what I call a '*layered approach*'—to the blunt tools currently used to delineate the extraterritorial scope of data privacy laws, such as that of the proposed EU Regulation.

A few words about the EU's proposed approach to extraterritoriality in data privacy law

As noted, Moerel, and others, have already described and discussed the complex, yet unsophisticated, approach to extraterritoriality taken in the EU Data Protection Directive.[7] Here, I will restrict the discussion to a brief introduction to the approach taken in the proposed Regulation.

Apart from one very serious flaw, the approach to extraterritoriality found in the January 2012 proposal for a *General Data Protection Regulation*[8] is an improvement on the approach taken in the Directive. In more detail Article 3 reads as follows:

1. This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union.
2. This Regulation applies to the processing of personal data of data subjects residing 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 to such data subjects in the Union*; or

   (b) *the monitoring of their behaviour.*

4. This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where the national law of a Member State applies *by virtue of public international law.* (emphasis added)

The flaw I alluded to is that, while the rule articulated in Article 3(2)(a) contains a double requirement; that is, (1) the data subject must reside in the European Union (similar to passive nationality), and (2) the conduct must take place in the EU (similar to objective territoriality), Article 3(2)(b), which must be read independently from Article 3(2)(a), only contains the first requirement—it only focuses on whether the data subject resides in the European Union. As I pointed out in a blog post of 24 March 2013,[9] this suggests that EU residents enjoy the protection of the Regulation worldwide simply by residing in the European Union. In the absence of further restrictions, this protection would then seem to attach to the very person of EU residents so as to enable them also to rely on this protection when travelling outside the EU—an unrealistic outcome that would bring some legitimacy to claims of a European 'data privacy imperialism'.

While otherwise largely unchanged, this flaw has been addressed in the (at the time of writing) latest roll of the dice in the progress towards a European Data Protection Regulation; that is, the draft compromise text of the Irish Presidency of the Council of the European Union's Justice and Home Affairs.[10]

The result, at least so far, is that the proposed approach to extraterritoriality of the future Regulation is in line with, or an improvement on, the absolute majority of data privacy laws with extraterritorial application around the world. Nevertheless, it is my view that we can find a solution that provides greater fairness in the form of extraterritorial data protection where, and only where, such data protection is justified.

A 'layered approach'

As data privacy laws always incorporate a diverse range of legal rules, we need to dissect each such piece of legislation and identify the different types of rules they include. For example, most data privacy laws contain provisions seeking to discourage, or even penalize, unauthorized and unreasonable disclosure or other use of

5 Kuner et al., 'Editorial' (n 3) 147.

6 Christopher Kuner, *Transborder Data Flows and Data Privacy* (Oxford: Oxford University Press 2013). See in particular ch. 6.

7 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, Official Journal (L 281).

8 *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*, COM (2012) 11 (25 Jan. 2012).

9 Dan Svantesson, The territorial scope of the proposed EU Data Protection Regulation, blawblaw.se (24 March 2013) <http://blawblaw.se/2013/03/the-territorial-scope-of-the-proposed-eu-data-protection-regulation/> accessed 1 Aug. 2013.

10 As reported at: huntonprivacyblog.com <http://www.huntonprivacyblog.com/wp-content/uploads/2013/06/st10227-ad01.en13.pdf> accessed 1 Aug. 2013.

www.manaraa.com

personal data. Such provisions are similar in nature to rules found in other areas of law, such as the law of defamation. In a sense, they are private in nature and, therefore, fundamentally different to some other types of rules found in some data privacy laws, such as requirements of a designated Data Protection Officer,[11] that are of a public law nature.

In light of this, it is simply not productive of good results to view the question of extraterritorial claims from the perspective of whether they should be allowed or not in relation to data privacy laws. Indeed, it is not sufficient to ask when such claims are justified in relation to data privacy laws. We need to take one step further and introduce a further level of nuances and sophistication—we need a '*layered approach*' taking account of the multifaceted nature of substantive data privacy law.

For example, while it may be reasonable to ask a foreign company to abide by a country's abuse-prevention rules (such as rules discouraging or penalizing unauthorized and unreasonable disclosure or other use of personal data) based on a certain degree of contact between that company and that country (eg, a transaction involving the collection of personal data), the same degree of contact may not justify that country imposing on the company the duty of designating a Data Protection Officer.

Thus, the key to balance and reasonableness in the field of extraterritoriality in data privacy law lies in matching the various provisions found in each data privacy law to suitable criteria for their extraterritorial application.

As often is the case with complex tasks, this particular task may be carried out in more than one way. Here, I will perform the task in two steps. First, I will discuss what types of substantive data privacy rules ought to be fitted within each layer of extraterritorial claims. Second, I will construct suitable limitations on the extraterritorial reach of each of these different layers.

Matching substantive data privacy law rules to the layers of extraterritorial claims

In an attempt to strike a balance between usability and sophistication, I have opted for a model with three different layers of extraterritorial claims. However, I acknowledge that, despite its prevalence in western fairy-tale tradition, there is no magic in the number three and that one could picture a model with any number of layers from two upwards.

In any case, for my model I have chosen to refer to my three layers as follows:

1. The abuse-prevention layer;
2. The rights layer;
3. The administrative layer.

I will not here seek to dissect every single data privacy law and identify which provisions fit into which layer. Indeed, I hasten to add that such an exercise is by no means free from subjectivity. However, a few illustrative examples can usefully be presented.

As already noted, data privacy laws commonly contain provisions seeking to discourage or to penalize unauthorized and unreasonable disclosure or other use of personal data, in a manner similar to how, for example, defamation law seeks to prevent abuse. Such rules ought to fall clearly within the abuse-prevention layer.

Within the rights layer we can comfortably place data privacy rules such as the right of access and the right of correction commonly found in data privacy laws.

As already hinted, in the administrative layer we should place data privacy rules such as the requirements of a designated Data Protection Officer[12] found in the proposed EU data privacy Regulation.

I confess that, in the above, I have taken the easy option of focusing on data privacy rules that are relatively easy to place within the different layers, and thus, I could be accused of 'hiding behind easy examples'. Further, I acknowledge that not all substantive data privacy rules may be so easily sorted into the three layers. Thus, in order to also engage with some of the more complicated, and subjective, choices that need to be made, I provide a table of substantive data privacy rules sorted into my three layers (Table 1). In doing so, I draw upon examples from the OECD 1980 *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* and from the proposed EU Regulation.

On a practical level, perhaps the greatest hurdle to overcome in organizing the substantive data privacy rules into these three layers is found in the fact that certain such substantive rules, and even more so certain Articles of substantive rules, incorporate matters that may fall within different layers. I do not strive to address that concern here, but note that the solution ought to be found in the structuring of the substantive rules and Articles as such. In other words, it may be that a

11 See eg *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals* (n 8), art. 35(1).

12 See eg *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals* (n 8), art. 35(1).

www.manaraa.com

Table 1. Examples of substantive data privacy rules sorted into three proposed layers

Substantive data privacy rule	Layer
OECD's Collection Limitation Principle[a]	Abuse-prevention
OECD's Data Quality Principle[b]	Rights
OECD's Purpose Specification Principle[c]	Abuse-prevention
OECD's Use Limitation Principle[d]	Abuse-prevention
OECD's Security Safeguards Principle[e]	Rights
OECD's Openness Principle[f]	Rights
EU Regulation's rule on policy development[g]	Administrative
EU Regulation's rule on data protection by design and by default[h]	Administrative
EU Regulation's rule on data protection officers[i]	Administrative

Notes: [a]'There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.'
[b]'Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.'
[c]'The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.'
[d]'Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 [the Purpose Specification Principle] except: a) with the consent of the data subject; or b) by the authority of law.'
[e]'Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.'
[f]'There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.'
[g]'The controller shall adopt policies and implement appropriate measures to ensure and be able to demonstrate that the processing of personal data is performed in compliance with this Regulation.' *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals* (n 8), art. 22(1).
[h]'Having regard to the state of the art and the cost of implementation, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures and procedures in such a way that the processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject.' *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* COM (2012) 11 (25 Jan. 2012), art. 23(1).
[i]'The controller and the processor shall designate a data protection officer in any case where: (b) the processing is carried out by an enterprise employing 250 persons or more, or (c) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects.' *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regards to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* COM (2012) 11 (25 Jan. 2012), art. 35(1).

reorganization of the substantive rules and Articles is required in order that they may be fitted into the layers. This will no doubt be an onerous task requiring great sensitivity and insight.

On a theoretical level, the greatest hurdle to overcome in dividing the substantive data privacy rules into these three layers is found in the fact that we are dealing with a fundamental human right. Put differently, we may question the suitability, or indeed possibility, of splitting a fundamental human right into different layers of obligations. However, I think we may reasonably view the standard set by international human rights law as a minimum standard and I suspect we may see initiatives such as the proposed Regulation as going beyond that minimum standard. Thus, as long as the layering does not result in any instances of violations of that minimum standard, no problems should arise.

The extraterritorial reach of the three layers

Having outlined, albeit in a somewhat eclectic manner, the types of substantive data privacy law rules that ought to fit in each layer, these three layers are now discussed in order and proposals are made for how we can delineate their respective extraterritorial reach.

Owing to the similarity to, for example, defamation law, data privacy law provisions falling within the

www.manaraa.com

abuse-prevention layer may reasonably be given an equally broad extraterritorial application as defamation law typically is given. Without engaging in a full-scale analysis of the extraterritorial reach of defamation laws, it is undeniable that defamation law is commonly applied in a wide jurisdictional manner.[13] At the same time, even a cursory examination of cross-border Internet defamation cases makes clear that the search for a broadly accepted approach is still on.[14] Consequently, we are not restricted here to adopting the jurisdictional delineation applied in defamation disputes.

I argue that for the abuse-prevention layer, we may apply an unrestricted version of the doctrine of 'market sovereignty' that I have presented elsewhere.[15] Put briefly, a state has market sovereignty, and therefore justifiable jurisdiction, over Internet conduct where it can effectively exercise 'market destroying measures' over the market that the conduct relates to. Market destroying measures include, for example, substantive law allowing its courts, due to the foreign party's actions and subsequent refusal to appear before the court, to make a finding that:

- that party is not allowed to trade within the jurisdiction in question;
- debts owed to that party are unenforceable within the jurisdiction in question; and/or
- parties within the control of that government (eg residents or citizens) are not allowed to trade with the foreign party.

Thus, a country ought to be free to apply the parts of its data privacy law that fall within the abuse-prevention layer in an extraterritorial manner as soon as it has market sovereignty over the market to which the conduct relates. Essentially, this means that extraterritorial jurisdiction is possible as soon as a foreign controller collects data from an EU resident present in the EU, and one could imagine alternatives to the proposed reliance on the doctrine of market sovereignty that would produce a substantially similar result.

When we turn to the rights layer—layer two—it is clear that we can no longer rely on 'binary tests' such as the test applied for the abuse-prevention layer. We need a test that takes account of the degree of contact between the object (eg a foreign company) and the country seeking to exercise jurisdiction in an extraterritorial manner.

Here it is useful to pause to consider the inadequacy of the grounds for jurisdiction typically put forward in international law, and most prominently through the well-known *Harvard Draft*.[16] None of the grounds for jurisdiction outlined in the *Harvard Draft* take account of the degree of contact. Instead they focus on binary measures such as whether the offender[17] or victim was within the territory of the country claiming jurisdiction or not[18] and on whether the offender is a national of that country or not.[19] Such rules are, due to their lack of sophistication, doomed to produce unacceptable outcomes when applied to complex scenarios. Thus, the answer to the question of what test we may apply to the rights layer is not to be found in the grounds for jurisdiction typically put forward in international law.

To find an appropriate test for layer two—the rights layer—claims of extraterritorial jurisdiction we should instead turn to basic principles from US law of long-arm jurisdiction, and more specifically to the familiar 'minimum contact' test first formulated in *International Shoe Co. v Washington*:[20]

> [D]ue process requires only that in order to subject a defendant to a judgment in personam, if he be not present within the territory of the forum, he have certain *minimum contacts* with it such that the maintenance of the suit does not offend '*traditional notions of fair play and substantial justice*.'[21]

The reason for what were at that time new jurisdictional rules, stated in *International Shoe Co. v Washington*, was the aim of an adjustment to a more mobile society—an aim of even greater importance today with our significantly more mobile society.

Since the case was decided on 3 December 1945, the factors taken into account in the test have changed somewhat, and different courts have interpreted the *International Shoe Co. v Washington* case differently. That does not, however, impact its use here as I am not proposing an adoption of the exact test as such. Rather, what I am proposing is that the idea of a minimum contact test is also useful for delineating the extraterritorial reach of the substantive data privacy rules that fall within the rights layer.

13 See eg the High Court of Australia case of *Dow Jones & Company Inc. v Gutnick* (2002) 210 CLR 575 and the ECJ joined cases of *eDate Advertising GmbH v X* and *Olivier Martinez and Robert Martinez v MGN Limited* C-509/09 and C-161/10.

14 See eg Dan Svantesson, *Private International Law and the Internet* (2nd edn, Kluwer Law International, Alphen aan den Rijn, 2012).

15 Dan Svantesson, *Extraterritoriality of Data Privacy Law* (forthcoming, Ex Tuto Publishing, Copenhagen, 2013).

16 1935 *Harvard Research Draft Convention on Jurisdiction with Respect to Crime*.

17 The so-called subjective territoriality principle.

18 The so-called objective territoriality principle.

19 The so-called nationality principle.

20 *International Shoe Co. v Washington*, 326 U.S. 310 (1945).

21 *International Shoe Co. v Washington*, at 316 (emphasis added).

www.manaraa.com

Having said that, important guidance can be gained from one of the most important cases examining the minimum contact test—*Hanson v Denckla*.[22] In that case, the Court stated that it is always necessary that there be an act 'by which the defendant purposefully avails itself of the privilege of conducting activities within the forum State, thus invoking the benefits and protections of its laws',[23] for a minimum contact to be established.[24] This reasoning may also be usefully adopted for the minimum test for layer two.

Turning to the search for a suitable test for the administrative layer, we again need a test that is more sophisticated than the binary tests of the *Harvard Draft*, and we may once more draw upon ideas and concepts found in the basic principles of US law on jurisdiction. More specifically, to properly account for the onerous nature of the substantive data privacy rules that fall within the administrative layer—layer three—we must ensure that the test we apply is indeed strict, and we can benefit from looking to how the United States has dealt with the so-called 'general jurisdiction' of courts. Under US law, general jurisdiction may be exercised when a party's ties to the forum are continuous, systematic, and ongoing.[25] This is measured by reference to the quality and quantity of the defendant's contacts with the forum.[26] As noted, for example, by Jensen, this means that a fairly high standard must be met: 'To assert general jurisdiction over an out-of-forum defendant, a court must find that the defendant's minimum contacts with the forum are so systematic that they serve as a proxy for physical presence.'[27] Furthermore, '[e]ven if substantial, or continuous and systematic, contacts exist, the assertion of general jurisdiction must be reasonable'.[28]

There are a limited number of US cases relating to the assertion of general jurisdiction in an international context, one of the most well-known being *Helicoptoros Nacionales De Columbia S.A. v Hall*.[29] In that case, the Supreme Court of the United States denied a Texas Court the right to assert jurisdiction over a non-resident defendant. The contact between the state of Texas and the defendant included the following:

- the contract pursuant to which the defendant provided the transportation service being used at the time of the crash was negotiated in Houston, Texas;
- 80 per cent, or $4,000,000 US dollars' worth, of the defendant's fleet of helicopters were purchased from Bell Helicopters Company in Fort Worth, Texas; and
- the defendant sent its prospective pilots, management, and maintenance personnel to Fort Worth, Texas, for training purposes.

Although it could be argued that these facts indicate an ongoing continuous and systematic contact with the state of Texas, the Court held against the assertion of general jurisdiction. This was motivated by a range of factors, the most noteworthy being that 'mere purchases, even if occurring at regular intervals, are not enough to warrant a State's assertion of in personam jurisdiction over a non-resident corporation in a cause of action not related to those purchase transactions'.[30]

Since there was some form of ongoing continuous and systematic contact with the forum state in this case, one must ask why the assertion of general jurisdiction was not upheld. While it is possible that the 'reasonableness' influenced the Court, this case illustrates that ongoing, continuous and systematic contacts must fulfil some form of 'substantiality requisite'—there must be a certain degree of substantiality to the ongoing continuous and systematic contact between the forum and the case at hand.

To conclude this part of the discussion, I propose that the test for the extraterritorial application of the substantive data privacy rules that fall within the administrative layer should be focused on whether the object's contacts with the country claiming jurisdiction are sufficiently substantial, continuous, and systematic, making the exercise of extraterritorial jurisdiction reasonable. This proposal does, however, not amount to an adoption of the US concept of general jurisdiction as such. It merely draws upon the test developed for the purpose of delineating US general jurisdiction.

Importantly, none of the tests in the three layers are comparative; that is, there is never any need to consider whether a particular matter is more closely connected to another forum. Thus, all three tests are distinctly unilateral in nature, which ought to simplify their application in practice.

Furthermore, it is relevant to note that organizations (eg from the United States) wishing to avoid Internet-based contact with persons from certain countries or

22 *Hanson v Denckla*, 357 U.S. 235 (1958).

23 *Hanson v Denckla*, at 253.

24 *Hanson v Denckla*, at 253.

25 *Helicoptoros Nacionales De Columbia, S.A. v Hall*, 466 U.S. (1984).

26 *Phillips Exeter Acad. v Howard Phillips Fund, Inc.*, 196 F.3d 284, 288 (1st Cir. 1999).

27 JM Jensen, *Personal Jurisdiction in Federal Courts over International E-Commerce Cases* 40 Loy. L. A. L. Rev. 1507, 1521 (2006–7).

28 *Gator.com Corp. v L.L. Bean*, 03 C.D.O.S. 7986, 2003 US App. LEXIS 18115 (9th Cir. 2 September 2003) referring to *Amoco Egypt Oil Co. v Leonis Navigation Co, Inc.*, 1 F.3d 848, 852–853 (9th Cir. 1993).

29 *Helicoptoros Nacionales De Columbia, S.A. v Hall*, 466 U.S. (1984).

30 *Helicoptoros Nacionales De Columbia, S.A. v Hall*

www.manaraa.com

regions with detailed data privacy laws (such as the European Union) may rely on so-called geo-location technologies to ascertain the geographical location of Internet users.[31] This means that the burden of taking active steps to avoid the type of contact that invokes the extraterritorial jurisdiction of countries with data privacy laws is manageable, if not neglectable.

One last matter must be addressed in this context. Geo-location technologies may produce inaccurate results including false positives and false negatives. False negatives are not of interest here, but we must ask what results may stem from false positives. For example, we may ask whether a foreign business that has implemented a geo-location technology specifically to avoid contact with customers from country A may still be bound by the substantive data privacy laws of country A in the event of contact with customers from country A resulting from the geo-location technology producing false positives. Given the degree of contact required for a extraterritorial claim under the administrative layer, we ought to be able to focus on the other two layers only.

Looking at the question of whether the foreign business in the example should be caught by the extraterritoriality of the rights layer, and/or of the abuse prevention layer, we can only find subjective answers. However, a few (relatively) objective observations may be made.

First, it seems beyond intelligent dispute that the foreign business in the example should only ever be shielded from extraterritoriality by the use of geo-location technologies where such a use takes place in good faith.

Second, the appropriateness of the type of geo-location technology used must be assessed on a case-by-case basis taking account of the individual circumstances of the case.

Third, bearing in mind the higher degree of contact required for the rights layer, it seems more appropriate that the use of geo-location technologies to dis-target customers from country A be viewed as a more effective means to exclude the extraterritoriality of the abuse prevention layer than of the rights layer. In other words, as the risk of occasional false positives is higher than the risk of systematic false positives, the probability of a degree of contact bringing into play the abuse prevention layer is greater than the probability of a degree of contact bringing into play the rights layer. Thus, it would seem more difficult to argue good faith where the degree of contact is such as to invoke the rights layer.

On the other hand, as the substantive data privacy rules of the abuse prevention layer merely aim to avoid abusive behaviour, it is arguably not too onerous a demand to request a foreign business collecting personal information from a customer from a country with which the business sought to avoid contact, to comply with those rules in relation to the personal information it collected as a result of a false positive.

A model Article applying the layered approach

At this stage it may be useful to try to summarize what has been said so far about the layered approach advocated here, in the form of an Article that could form part of data privacy legislation such as the proposed EU Regulation:

Article X[32]

1. The following Articles of this [Regulation] fall within layer one (the 'abuse-prevention layer'): [list relevant Articles].
2. The following Articles of this [Regulation] fall within layer two (the 'rights layer'): [list relevant Articles].
3. The following Articles of this [Regulation] fall within layer three (the 'administrative layer'): [list relevant Articles].
4. The Articles of this [Regulation] falling within layer one apply in an extraterritorial manner where [the Union] has market sovereignty over the [controller's] conduct, by reference to whether it can effectively exercise 'market destroying measures' over the market that the conduct relates to.
5. The Articles of this [Regulation] falling within layers one and two apply in an extraterritorial manner where a [controller] not established [in the Union] has certain minimum contacts with [the Union] for example by purposefully availing itself of the privilege of conducting activities within [the Union], thus invoking the benefits and protections of its laws.
6. The Articles of this [Regulation] falling within layers one, two and three apply in an extraterritorial manner where a [controller's] ties to [the Union] are sufficiently substantial, continuous and systematic to make the exercise of extraterritorial jurisdiction reasonable.

To this could be added a provision such as this:

7. This [Regulation] does not apply in an extraterritorial manner to a [controller] that, acting in good faith has taken reasonable steps to avoid contact with [the Union].

31 See eg Svantesson, *Private International Law and the Internet* (n 14).

32 Apart from the reference to 'list relevant Articles', the text in brackets is aimed directly at the EU context and should obviously be substituted where Article X is applied in other jurisdictions.

www.manaraa.com

This example is obviously only one possible way in which one may structure the type of layered approach I have canvassed. And admittedly, some aspects of this Article X could benefit from being fleshed out somewhat. Nevertheless, it is hoped that 'Article X' constitutes a useful illustration of the layered approach.

Finally, it should be noted that one could perhaps imagine the structure proposed above being introduced by the courts rather than by the legislature. However, for that to be possible, the legislative text, for example, the proposed EU Regulation, would presumably need to cater for such judicial creativity in some way.

A brief illustration of the layered approach's application

A few examples may usefully illustrate how the layered approach advocated in this paper would work on a practical level.

Imagine that company *Z*, based in the United States, enters into thousands of transactions with consumers in Europe every month, and that it directs a marketing campaign towards European consumers online, in European magazines, and on European TV stations. Imagine further that it undertakes no marketing activities towards Australia and only comes into contact with one Australian consumer who contacts the company to gain information about one of the company's products. Finally, imagine that company *Z* regularly enters into a small number of transactions with consumers in Singapore but does not in any sense target its activities towards Singaporean consumers.

In such a situation, it could be concluded that, under the layered approach outlined above, company *Z* would fall within all three layers in relation to EU data privacy law. Further, company *Z* would fall within the first two layers in relation to Singaporean data privacy law and only fall within the first layer—the abuse-prevention layer—in relation to Australian data privacy law.

While the model of a layered approach to extraterritoriality in data privacy law outlined here ought to have obvious benefits, it is also associated with at least one problem as can be illustrated in the following example.

Imagine that person *A* and person *B*, both residing in the EU, are considering buying a particular eBook. Person A does so from company *X* and person *B* does so from company *Y*. Imagine further that, while company *Y* deals with EU consumers to such a degree that it meets the minimum contact test of the rights layer, company *X* does not meet that test.

In this case, person *A* is then enjoying a lower level of protection (ie only abuse-prevention), while person *B* is enjoying a higher level of protection (ie both abuse-prevention and the rights of the rights layer). This difference in protection may be seen as unfair since, from the perspective of persons *A* and *B*, the level of protection they respectively receive must appear rather random; that is, persons *A* and *B* may not, at the time of interaction with companies *X* and *Y* respectively have known the extent to which those companies engage on the relevant market.

This disadvantage does not, however, substantially undermine the overall attractiveness of the model put forward here.

Concluding remarks

While a relatively recent phenomenon, the e-commerce industry has had time to witness a boom and a bust, as well as a recovery resulting in a relatively 'mature' industry. The United States, with Silicon Valley as a spearhead, has maintained a leadership role in e-commerce activities, with current figures showing e-commerce sales at a level of $59.54 billion.[33] Thus, any foreign regulations that impact on e-commerce, such as the data privacy laws in focus in this article, are of particular relevance for the United States. However, such laws obviously affect businesses around the globe and equally obviously do not only affect pure e-commerce businesses. Many, not to say most, businesses today have a presence online, and with such a presence comes an exposure to foreign data privacy laws.

To comply with all the data privacy laws a major company comes into contact with would require legal advice in relation to each of those laws, which is obviously costly, if not impossible. Attempts to minimize costs could be made by aiming at compliance with what is perceived as the strictest law, but such an approach presupposes that one law is stricter in all regards than the other laws. The reality is more likely to be that some laws are stricter in some regards while other laws are stricter in other regards.

At the same time, it is of course the case that, with the exception of the approach advocated in the form of the doctrine of market sovereignty, extraterritorial claims may often have limited practical implications due to the lack of any means of enforcement. While other factors enter the equation too, there is a correlation between the width of the claim and its likely enforceability in that the wider the claim the less likely its practical enforcement. This takes us deep into the realm of legal theory and philosophy as we need to confront the question of whether law may have a value even where it cannot be

33 *U.S. E-Commerce Sales: 59.54B USD for Q4 2012*, YCharts, <http://ycharts.com/indicators/ecommerce_sales> accessed 17 Jul. 2013).

www.manaraa.com

effectively enforced. Several theorists have discussed this important question, and scholars in data privacy law have also engaged with the issue. Bygrave, for example, has described 'regulatory overreaching' referring to 'a situation in which rules are expressed so generally and non-discriminately that they apply *prima facie* to a large range of activities without having much of a realistic chance of being enforced'.[34] He views such 'regulatory overreaching' as a problem:[35]—a view apparently embraced by several other leading commentators such as Maier,[36] Kuner[37] and Moerel.[38]

I have, however, argued that, in the context of the extraterritoriality of data privacy laws, what Bygrave terms 'regulatory overreaching' need not always be a problem, and that we need to distinguish between what we can call 'bite jurisdiction' on the one hand and 'bark jurisdiction' on the other.[39] I argue that there may well be solid reasons why a state may wish to make clear its standpoint on a particular issue by legislating against it even though the effective enforcement of the law in question may be difficult, cumbersome or, indeed, unlikely.[40]

In any case, this article has argued that the difficulties created by the extraterritorial application of data privacy laws could be addressed if we introduce a more sophisticated delineation of the extraterritorial scope of such laws—the current use of binary tests determining, in a one size fits all manner, whether a data privacy law, with all its distinctly different types of rules, applies or not, and is productive of unfair results.

A layered approach applying sophisticated delineations of extraterritorial reach could considerably improve the situation and should be adopted for the proposed EU Regulation, as well as in other data privacy laws.

doi:10.1093/idpl/ipt027
Advance Access Publication 20 September 2013

34 Lee Bygrave, 'Determining Applicable Law Pursuant to European Data Protection Legislation' (2000) 16 *Computer Law and Security Report* 252, 255.

35 Bygrave, 'Determining Applicable Law (n 34).

36 Bernhard Maier, 'How Has the Law Attempted to Tackle the Borderless Nature of the Internet?' (2010) 18(2) *International Journal of Law and Information Technology* 161.

37 Christopher Kuner, 'Data Protection Law and International Jurisdiction on the Internet (Part 2)' (2010) 18(3) *International Journal of Law and Information Technology* 227, 235.

38 Lokke Moerel, 'The Long Arm of EU Data Protection Law: Does the Data Protection Directive Apply to Processing of Personal Data of EU Citizens by Websites Worldwide?' (2011) 1(1) *International Data Privacy Law* 23, 24.

39 See further: Svantesson, *Extraterritoriality of Data Privacy Law* (n 15).

40 For example, the Article 29 Working Group has noted that 'there exist examples that the foreign web site may nevertheless follow the judgement and adapt its data processing with a view to developing good business practice and to maintaining a good commercial image [even where third countries will not recognise and enforce the judgement]': Article 29 Working Group, *Working Document on Determining the International Application of EU Data Protection Law to Personal Data Processing on the Internet by Non-EU Based Web Sites* (Working Paper 56, adopted 30 May 2002) 15.

www.manaraa.com

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.

www.manaraa.com