EXTRATERRITORIALITY IN THE CONTEXT OF DATA PRIVACY REGULATION

by

DAN JERKER B. SVANTESSON*

An examination of current and proposed regulatory initiatives relating to data privacy shows a tendency of extraterritorial jurisdictional claims. While there is nothing novel about extraterritorial jurisdictional claims as such, the impact they have in the data privacy setting is largely unexplored. This paper discusses extraterritorial jurisdictional claims found in a selection of current and proposed regulatory initiatives relating to data privacy. Special attention is given to how such claims affect, and are affected by, modern use of information and communication technologies.

KEYWORDS
extraterritoriality; jurisdiction; data privacy; data protection

1. INTRODUCTION

It may well be the case that extraterritorial jurisdictional claims have been made for as long as the world has been divided into different jurisdictions. However, it is plain to see that the need for such extraterritorial claims is directly related to the extent of cross-jurisdictional interactions. Thus, a bit simplified, it can be said that, with a higher frequency, as well as with a greater significance, of cross-jurisdictional interactions, comes a greater incentive for states to exercise extraterritorial jurisdiction.

Modern society caters for a considerable degree of cross-jurisdictional interactions. In fact, we are witnessing a degree of such interaction unimagin-

* 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.

able just 30 years ago. International calling rates are dropping, international flights are prices so as to make it possible for most people in developed countries to engage in international travel, and then there is the most important component of them all – the Internet.

As has been pointed out, in various ways, in the introduction of virtually every single law journal article dealing with Internet cross-border issues, the Internet makes possible an effortless cross-border communication where distance plays only a very minor role (even though the importance of location remains).[1]

In light of the above, it can be said that never before, in the history of mankind, have the incentives for extraterritorial jurisdictional claims been stronger. And it is against this backdrop that this article proceeds to discuss extraterritorial jurisdictional claims found in a selection of current and proposed regulatory initiatives relating to data privacy.

2. THE INTERNATIONAL DIMENSIONS OF DATA PRIVACY

Since the 1960s, data privacy regulations have increasingly been introduced around the world.[2] This is not surprising considering the important role data plays in modern society. In fact, no sensible person would dispute that the importance of data, including personal data, will only continue to increase in the foreseeable future.

Those seeking to formulate data privacy regulation have traditionally engaged with two separate questions of a cross-border nature:

1. Under what circumstances may data be transferred out of the jurisdiction; and

2. Under what circumstances will extraterritorial jurisdiction be claimed?

The first of these questions has gained a considerable amount of attention, not least as of late.[3] However, the second question – relating to

---

[1] Svantesson, D. 2012, 'Time for the law to take Internet geo-location technologies seriously', Journal of Private International Law, vol. 8, no. 3, pp. 473-487.

[2] For interesting overviews of current data protection regulations, refer to: Greenleaf, G. 2012, 'The Influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108' International Data Privacy Law, vol. 2, no. 2; and Greenleaf, G. 2012, 'Global Data Privacy Laws: 89 Countries, and Accelerating', Privacy Laws & Business International Report, iss. 115, Special Supplement.

[3] Refer e.g. to the works of Christopher Kuner who has written extensively and in detail on this topic, see e.g. his forthcoming PhD on the topic. See also e.g.: Svantesson, D. 2011, 'Fundamental policy considerations for the regulation of Internet cross-border privacy issues', Policy & Internet, vol. 3(3), no. 7.

extraterritorial claims of jurisdiction – has largely been ignored.[4]

3. EXAMPLES OF EXTRATERRITORIAL JURISDICTIONAL CLAIMS

In the area of data privacy regulation, as well as in other related areas of law, there appears to be a trend towards an increase in extraterritorial jurisdictional claims. However, some states have somewhat of a tradition of making such extraterritorial claims. In Australia, for example, the *Privacy Act 1988* (Cth) contains, in section 5B, rules giving extraterritorial application to the Act in relation to:

- acts or practices relating to personal information about an Australian citizen or some others treated equally to Australian citizens in this setting;
- Australian organisations;
- organisations that carry on business in Australia; or
- situations where the personal information was collected or held by the organisation in Australia or an external Territory, either before or at the time of the act or practice.[5]

As most readers of this journal would be aware, current EU data protection law also caters for extraterritorial claims. Article 4 of the relevant Directive makes clear that:

> 1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:
> […]
> (b) the controller is not established on the Member State's territory, but in a place where its *national law applies by virtue of international public law*;
> (c) 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

[4] Some notable work has, however, been done in this area, such as the following excellent articles: Coughlan, S., Currie, R., Kindred, H., and Scassa, T. 2007, 'Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization' Canadian Journal of Law and Technology vol. 6, pp. 29-60; Kuner, C. 2010, 'Data Protection Law and International Jurisdiction on the Internet (Part 1), International Journal of Law and Information Technology, vol. 18, p. 176, and Bygrave, L. A. 2000, 'Determining Applicable Law Pursuant to European Data Protection Legislation, Computer Law and Security, vol. 16, no. 4, p 252.

[5] This, admittedly simplified, description relates to Australian law as it stands prior to the substantial reform in progress at the time of writing.

> through the territory of the Community.[6] (emphasis added)

The reference to the making use of "equipment, automated or otherwise, situated on the territory" possesses a somewhat mystical character and has proven difficult to apply in the Internet setting. In the proposed EU data protection Regulation, this approach has been abandoned in favour of the following found in the Regulation's Article 3:

> 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*.
>
> 3. 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)

Interestingly, and no doubt controversially, this provision seems 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.

Another example of recent developments in data privacy law taking an expansive extraterritorial approach is found in the recently enacted *Personal Data Protection Act 2012* in Singapore. This Act "will apply to organisations in Singapore and those that are engaged in data collection, processing or disclosure of data of individuals within Singapore, even if the organisation is not physically located in Singapore."[7] It is noteworthy that, in discussing the extraterritorial dimension of the Act, the Ministry of Information, Communications and the Arts (MICA) observed that:

> MICA is cognisant of the implementation challenges. In particular, where the organisation in question has no presence in Singapore, it would be difficult to carry out investigations into any complaint made in relation to an activity of the organisation, or to proceed with any enforcement action against the organisation. However,

---

[6] 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 O.J. (L 281) 31.

[7] Sheena Jacob and Jinesh Lalwani, Personal Data Protection law is enacted in Singapore (18.10.12) http://www.twobirds.com/English/News/Articles/Pages/personal_data_protection_law_is_enacted_in_singapore_1012.Aspx (last accessed 30 December 2012).

> such coverage would act as deterrence for overseas companies to engage in activities that might result in a breach of the PDPA, and provide consistent treatment for local vis-a-vis overseas organisations with data-related operations in Singapore.[8]

Looking at other relevant recent developments in related areas of law, it is worth observing the Philippines' *Cybercrime Prevention Act of 2012*[9] which was approved by the President on 12 September 2012. Covering a range of criminal activities of particular importance online, such as Internet defamation, this Act makes a wide jurisdictional claim through its section 21 which reads as follows:

> The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act. including any violation committed by a Filipino national regardless of the place of commission. Jurisdiction shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines. There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.[10]

The extraterritorial dimensions of this Act will, provided they are actually pursued, doubtlessly give rise to controversies.

4. A FEW WORDS ABOUT THE CONCEPT OF EXTRATERRITORIALITY

The above has demonstrated beyond reasonable doubt that countries do in fact make extraterritorial jurisdictional claims in the context of data privacy regulation and related fields such as online defamation. However, to further the discussion, it is necessary to delve into a somewhat deeper discussion of the concept of extraterritoriality.

4.1 THE FOUR TYPES OF JURISDICTION

First of all, it is useful to adopt the customary distinction between different forms of jurisdiction. That is the distinction between:

1. Prescriptive (or legislative) jurisdiction;

---

[8] Public Consultation Issued by Ministry of Information, Communications and the Arts – Proposed Personal Data Protection Bill (19 March 2012) http://app.mica.gov.sg/Data/0/Consultation%20Paper%20for%20PDP%20Bill.pdf (last accessed 30 December 2012).

[9] Republic Act No. 10175, *An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefore and for Other Purposes*.

[10] *Cybercrime Prevention Act of 2012*, Section 21.

2. Investigative jurisdiction;
3. Judicial (or adjudicative) jurisdiction; and
4. Enforcement jurisdiction.

Prescriptive (or legislative) jurisdiction relates to the power to make law in relation to a specific subject matter.

The second type of jurisdiction included above – investigative jurisdiction – is rarely, if ever, included in its own right in outlines of the various forms of jurisdiction,[11] but ought to be so included. It relates to the power to investigate a matter and must be kept separate from the jurisdiction to make rules, adjudicate disputes and to actually enforce the law. The instances where investigative jurisdiction plays a central role are numerous in the context of data privacy law and in areas such as consumer protection – areas where complaints often are best pursued by bodies such as privacy commissioners/ombudsmen and consumer protection agencies.

Judicial (or adjudicative) jurisdiction, as the name suggests, deals with the power to adjudicate a particular matter.

Finally, enforcement jurisdiction relates to the power to enforce the law put in place, in the sense of, for example, arresting, prosecuting and/or punishing an individual under that law.

All of these forms of jurisdiction may be exercised in an extraterritorial manner.

4.2 CAN, CAN, SHOULD?

Whichever form of jurisdiction we are dealing with, a state considering an extraterritorial approach needs to break down its decision-making process into at least three parts. First it should investigate whether its domestic laws allow for an extraterritorial claim to be made; that is, *can* it be done under domestic law? Second, it should examine whether support for the extraterritorial claim can be found in international law – *can* it be done under international law? Finally, the state should consider whether it *should* pursue the extraterritorial claim in light of factors such as:

- What can be achieved through the extraterritorial claim?
- How will such a claim impact upon other states?
- How will those other states react to that impact?
- What advantages can be gained?
- What negative results may follow?

In examining these policy questions, it should be noted that, excessive

[11] See e.g. Coughlan, S., Currie, R., Kindred, H., and Scassa, T. 2007, 'Global Reach, Local Grasp: Constructing Extraterritorial Jurisdiction in the Age of Globalization' Canadian Journal of Law and Technology vol. 6, p. 32, preferring the conventional three categories, including investigative jurisdiction as a component of enforcement jurisdiction.

jurisdictional claims by democratic countries undermines those countries' objections to such claims made, for example,. by oppressive dictatorships.

4.3 JURISDICTIONAL CLAIMS RECOGNISED UNDER INTERNATIONAL LAW

Anyone with an interest in jurisdictional issues will have come across the following 'grounds' for jurisdiction in international law:

> *Subjective territoriality principle* – the principle that jurisdiction can be exercised over acts that are carried out within the territory (e.g. a hunter in Sweden fires a shot, killing a man in Norway – Sweden can claim jurisdiction based on the subjective territoriality principle);
>
> *Objective territoriality principle* – the principle that jurisdiction can be exercised over acts that cause harm within the territory (e.g. a hunter in Sweden fires a shot, killing a man in Norway – Norway can claim jurisdiction based on the objective territoriality principle);
>
> *Nationality principle* – the principle that jurisdiction can be exercised over acts wherever they are carried out, if carried out by nationals of the country claiming jurisdiction (this principle has gained increasing popularity e.g. in legislation relating to child sex tourism, allowing states to punish such severe crime wherever it occurs if carried out by nationals of the country claiming jurisdiction);
>
> *Passive personality principle* – the principle that jurisdiction can be exercised over acts wherever they are carried out, if they cause harm to nationals of the country claiming jurisdiction;
>
> *Protective principle* – the principle that jurisdiction can be exercised over acts wherever they are carried out, if they pose a threat to central interests such as national security; and
>
> *Universal principle* – the principle that jurisdiction can be exercised, by any state, over acts wherever they are carried out, if the act in question is deemed to be offensive to the international community at large (examples include war crimes, piracy and genocide).

It is important not to forget that these principles, while universally (or virtually universally) included in public international law literature, (1) were identified more than 75 years ago, (2) at least originally, "deals only with penal jurisdiction and with particular offences",[12] and (3) stem from an academic research project.[13]

One interesting observation that can be made at this stage is that, states

[12] 'Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime 1935' American Journal of International Law, vol. 29, no. 443, p. 446.

today, generally, do not make wider jurisdictional claims than in the past. However, due to advances in technology and travel (globalisation), the reach of their jurisdictional rules has been extended.

Interestingly the type of extraterritorial claims found in the context of data privacy seem to fall within the controversial passive personality principle, or alternatively within the less controversial objective territoriality principle. For example, Article 4 of the current EU Data Protection Directive – through its focus on the geographical location of relevant equipment – could be argued to relate to the objective territoriality principle. In contrast, Article 3 of the proposed EU data protection Regulation – in placing focus, for example, on the behavioural monitoring of EU residents – seem more likely to fall within the controversial passive personality principle. This should lead to at least two conclusions. First, law makers may wish to frame their extraterritorial claims in a language that places those claims in the least controversial category possible. And second, the fact that extraterritorial claims, of the same nature and with the same practical implications, can be worded so as to be seen to fit within jurisdictional grounds of varying degrees of controversy suggest a flaw in the categorisation of jurisdictional grounds outlined above. At the minimum, it suggests that we need to be careful in how those categories are used.

4.4 RESPONSES TO EXTRATERRITORIAL JURISDICTIONAL CLAIMS

As can be expected, where one state perceives that another state makes extraterritorial claims of jurisdiction that are too wide, the first state may well decide to take protective steps. Such protective steps may be ineffective, measured or excessive and not all people will always agree on in which category particular such steps fall.

While I will not go into details, it is well known that the US for some time has been troubled by what it sees as libel tourism in foreign courts, particularly courts in the UK. Sparked by the peculiar *Ehrenfeld* case,[14] the US introduced legislative measures to combat libel tourism.[15] Most interestingly, in 2010 the Federal SPEECH Act – the *Securing the Protection of our Enduring and Established Constitutional Heritage Act*[16] – was introduced.

---

[13] 'Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime 1935' American Journal of International Law, vol. 29, no. 443, p. 445.

[14] [2005] EWHC 1156 (QB).

[15] For a fascinating account of this development and its broader context, see: Tweed, P. 2012, Privacy and Libel Law – The Clash with Press Freedom, Bloomsbury Professional Ltd, Haywards Heath. See also, the *Libel Terrorism Protection Act 2008 (N.Y.).*

[16] HR 2765.

That Act makes mandatory the nonrecognition of foreign defamation judgments that are viewed as being inconsistent with the First Amendment's protection of free speech.

The impact that this approach will have is difficult to predict at the time of writing. Yet, there can be no doubt that it sends a strong message to the rest of the world that the US does not trust other courts to adjudicate in defamation matters. The obvious risk is that this initiative prompts the response that other countries implement similar nonrecognition legislation in areas of law for which they do not trust adjudication by US courts. With such a development we will unfortunately witness a downward spiral effect in cross-border judicial cooperation.

An important lesson we can learn from this is that the wider the jurisdictional claims made by one state, the more likely and justifiable are the non-enforcement measures taken by other states.

5. CONCLUSIONS

From all this we can learn at least one thing: it is not uncommon that states make extraterritorial jurisdictional claims in areas such as data privacy and related fields. This gives rise to several questions. Importantly, we may ask whether it is reasonable for states to make such claims. And it is in the answer to that question we find the key problem in this area – extraterritorial jurisdictional claims are both reasonable and unreasonable.

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. That is; protection must be afforded whatever the geographical source of the attack. In fact, as I have highlighted elsewhere, Article 17(2) of the United Nation's International Covenant on

Civil and Political Rights appears to be a source of international law, requiring signatory states to make fairly wide jurisdictional claims in relation to the protection of the privacy of people within their jurisdiction or territory. This is because each signatory state has an obligation to provide legal protection against unlawful attacks on the privacy of people subject to its jurisdiction and those present within its territory, *regardless of the origins of the attacks*.[17]

[17] Svantesson, D. 2011 'Fundamental policy considerations for the regulation of Internet cross-border privacy issues', Policy & Internet, vol. 3, no. 3, pp. 1 - 27.

Furthermore, a state's failure to apply law extraterritorially may risk causing a competitive advantage for businesses based outside that state that do not have to abide by the law in question. This, in a sense, punishes those businesses that do the right thing in complying with the law.

At the same time, extraterritorial jurisdictional claims are 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.

Finding a method for balancing these competing interests will not be easy. However, it is a task that we no longer can avoid engaging with.