The territorial scope of the proposed EU Data Protection Regulation

A wake-up call for Australia

Svantesson, Dan Jerker B

Published in:
Internet Law Bulletin

The territorial scope of the proposed EU Data Protection Regulation — a wake-up call for Australia

Dr Dan Jerker B Svantesson *BOND UNIVERSITY*

Key points

- Australian businesses must be made aware of the potential risk of exposure to foreign data privacy laws.
- The Australian legal community needs to develop expertise in foreign data privacy law.
- The proposed EU Regulation on data protection carries with it heavy penalties.
- As currently drafted, the EU Regulation on data protection has an extraordinarily far-reaching extra-territorial scope.

Introduction

As is well known, the European Union is currently seeking to reform its data protection framework through the introduction of a Regulation to replace the 1995 Data Protection Directive (95/46/EC). This development will affect the data privacy landscape worldwide, not least as the proposed General Data Protection Regulation carries with it fines of up to 2% of the offending enterprise's annual worldwide turnover.[1]

The Regulation has come under significant scrutiny from various quarters. However, one Article — Art 3, determining the proposed Regulation's territorial scope — has received limited attention. This is surprising, since, for any non-EU party, Art 3 is the single most important provision in the entire proposed Regulation — after all, nothing can be of a more fundamental importance than a provision that determines whether the substantive rules of the Regulation apply or not. This fact could scarcely have escaped the attention of the drafters.

The extraterritorial scope as per Art 3

In its current form, Art 3 reads as follows:

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.]

Anyone attempting to get clarification as to the exact meaning of this Article, and the underlying principles that have guided the drafters, will logically turn to the Explanatory Memorandum. Unfortunately, doing so is an utter waste of time. Depending on one's personal disposition, one will either be amused, be dumbfounded, or feel great despair in finding that, under the heading "3.4 Detailed explanation of the proposal", all that the Explanatory Memorandum states about Art 3 is this: "Article 3 determines the territorial scope of the Regulation." If this is the "detailed explanation of the proposal", we need the drafters to provide a "super-extended director's cut" version as well.

This lack of attention to a key provision, which more than any other needs to be discussed in detail, is puzzling. What is worse, even on a charitable interpretation of the situation, the failure to provide reasonable guidance as to Art 3 is negligent — arguably suggesting that inadequate attention has been given to the territorial scope of the Regulation. At worst, it seems that the drafters are seeking to avoid attention being directed at the enormously important effect of Art 3.

The consequences for Australia (and the rest of the non-EU world)

Interestingly — and no doubt controversially — whichever version of Art 3 is finally entering into force, 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. While this can be said to be the case already under the current EU approach to

extraterritoriality, it is submitted that the new approach, as found in the proposed Regulation, goes even further.

In more detail, the rule articulated in Art 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). However, Art 3(2)(b), which must be read independently from Art 3(2)(a), only contains the first requirement — it only focuses on whether the data subject resides in the European Union.

If this is correct, then Art 3(2)(b) suggests that EU residents enjoy the protection of the Regulation simply by residing in the EU. 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 to rely on this protection also when travelling outside the EU. For example, an EU resident on holiday on the Gold Coast of Australia would be protected by the proposed Regulation by virtue of the EU residence if an Australian "controller", not "established" in the Union, processes personal data of the EU resident as part of monitoring the EU resident's behaviour on the Gold Coast!

This result is so absurd, and so clearly inappropriate, that it cannot have been the drafters' intention. Thus, the proposed Regulation must be amended to address this issue — and, indeed, all that is required to depart from this unfortunate situation is to include, in Art 3(2)(b), the words "in the Union" in the manner done in Art 3(2)(a).

Indeed, some experts seem to take such an amendment to Art 3(2)(b) for granted. In expressing his views on the proposed Regulation, the European Data Protection Supervisor stated that:

> He considers that *the offering of goods and services or the monitoring of the behaviour of data subjects in the Union* makes much more sense and is more in line with the reality of global exchanges of information than the existing criterion of the use of equipment in the EU, under Article 4(1)(c) of Directive 95/46/EC. [Emphasis added.][2]

While this interpretation is sensible, it would be much more comfortable to have the text of Art 3(2)(b) amended so as to cement this interpretation beyond any doubt.

Not just the EU

Even leaving aside the extreme element of the proposed extraterritoriality of the proposed EU Data Protection Regulation highlighted above, it is clear that Australian businesses need to be aware of the risk of being exposed to EU data protection law when engaging with consumers in the EU.

It is, however, important to remember that the EU is far from alone in giving extraterritoriality to its data privacy law. Looking at our region, for example, both Singapore and Malaysia have opted for data privacy laws with extraterritorial application. This obviously complicates the situation further. Not only do Australian online businesses have to consider Australian law, but they also need to consider the laws of a range of different countries — laws that may be inconsistent or even contradictory. This places a heavy onus on the Australian legal community to be sufficiently informed of when and how foreign law may impact Australian businesses.

It is noteworthy that, in discussing the extraterritorial dimension of Singapore's Personal Data Protection Act 2012 (PDPA), 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, 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.[3]

Indeed, Australian data privacy law also has extraterritorial application. More precisely, in Australia, the Privacy Act 1988 (Cth) contains, in s 5B, rules giving extraterritorial application to almost the entire 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.

While the Privacy Act is being amended through the recently passed Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Cth), those changes do not alter the approach taken to the Act's extraterritoriality.

Concluding remarks

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, 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.[4]

Dr Dan Jerker B Svantesson
Professor and Co-Director
Centre for Commercial Law, Faculty of Law
Bond University (Australia)

Researcher
Swedish Law & Informatics Research Institute
Stockholm University
Dan_Svantesson@bond.edu.au

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.

Footnotes

1. Article 79(6).
2. European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the data protection reform package", 7 March 2012, p 17.
3. Ministry of Information, Communications and the Arts, *Public Consultation Issued by Ministry of Information, Communications and the Arts — Proposed Personal Data Protection Bill*, 19 March 2012, available at www.app.mica.gov.sg.
4. While one may legitimately question whether it *always* should be possible for businesses to engage in cross-border trade, most commentators would see value in cross-border trade as such. I will not here explore this matter further, but the exact value of cross-border trade and the circumstances under which such trade ought to be carried out obviously lie at the heart of any assessment of the underlying competing policy goals.