scripted

Volume 17, Issue 1, January 2020

# Book review: *Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens*

W Kuan Hon
Cheltenham: Edward Elgar, 2017. 488 pages. ISBN 978 1 78643 196 7. £110.00.

*Reviewed by Jiahong Chen**



DOI: 10.2966/scrip.170120.152

* Research Fellow in IT Law, Horizon Digital Economy Research, University of Nottingham, UK, jiahong.chen@nottingham.ac.uk.

One quality of a good scholarly work, I believe, is the ability to engage the reader with effective dialogues raising interests around the main research question, and then guiding the reader to the conclusion that they would have naturally come to with the facts and reasons presented. It does not necessarily take a "conversational" writing style to achieve such a sense of participation, but will certainly take a great deal of anticipation of what might puzzle a reader, as well as much deliberation on the best approach to an accessible study.

W Kuan Hon's *Data Localization Laws and Policy* represents an excellent example of how an academic title – which often goes at length on a serious topic – may maintain the balance between a remarkable degree of engagement and an objective, accurate, structural, and sometimes technical narrative. The book conducts a thorough investigation into one of the most important components of the EU's data protection law: Restrictions on transfers of personal data to third (non-EEA) countries.

A reader would find themselves well set up for an intellectually interesting journey, where some of the common, pressing, yet largely ignored issues are nicely sharpened into some well-structured research questions, and then all answered in a convincing manner. For example, I have always wondered why the case *Lindqvist* – in which the ECJ rules that the publication of a data subject's health details on the Internet does not constitute "transfer" of data – does not feel right to me. An explanation from the author goes:

> It cannot be right that personal data may be published freely if the intention was to make the data available to anyone anywhere, yet adequate protection/safeguards must be implemented if the intention was to make the data available only to people in limited third countries […] (p. 86)

Other issues particularly interesting to me (and perhaps my fellow readers as well) also include: How will the expanded territorial scope of the GDPR

(especially in relation to data controllers established outside the EEA) have an impact on the compliance and enforcement of the restrictions on data transfers? (pp. 47-54) Why do US-based service providers take the Safe Harbour (and now the Privacy Shield) so seriously even when obtaining user consent is not a practical issue for them? (pp. 213-216) Why is the number of law enforcement cases so minimal if the breaches of the restrictions are as serious as one might expect? (pp. 247-250).

These questions are answered throughout the eight chapters of the book. Chapter 1 opens by providing the technical background (regarding cloud computing) as well as the legal one (such as the key concepts and principles of the Data Protection Directive and the GDPR). Chapter 2 then identifies the policy goals of restricting exports of personal data through a historical lens, and concludes that it has been a major objective of international data protection instruments to prevent evasion of a jurisdiction's law. Different approaches have been developed, with various criteria relating to the duties of the data controller or recipient, or the legal protection afforded by the third country. With the anticircumvention objective in mind, Chapter 3 focuses on the legal concept of "transfer", which turns out to be an outdated, impractical, and fragmented approach based on the idea that data can be physically located in a jurisdiction, which is far from reality in both the case of website uses and that of cloud computing. The data location misconception is then further explained and challenged in Chapter 4 as one of the assumptions underpinning EU data protection law. This misconception has led to two consequent assumptions that a country's effective jurisdiction (and thus power or responsibility to ensure adequate protection) depends on the physical location of data, and therefore, that geographically restricting export of data can serve the objective of anticircumvention. It is based on these assumptions that, as analysed in Chapter 5, the EU data protection regime has adopted a series of mechanisms to ensure

adequate protection of personal data in third countries, including adequacy decisions by the Commission, several specific types of appropriate safeguards, and a list of derogations (e.g. consent). The high-profile EU-US Safe Harbour scheme and its replacement, the Privacy Shield, are also discussed in detail in this chapter. Based on these established facts, Chapter 6 answers the question of the extent to which compliance with the restrictions on data transfers to third countries has been achieved, and if breaches represent a serious issue, why law enforcement has been low so far. The amount of evidence presented in the enquiry of the Safe Harbour shows a significant likelihood that high volumes of breaches are taking place daily, yet there is a lack of enforcement actions against such breaches, probably due to a mix of impracticality to comply with and inability to enforce the restrictions. Against this backdrop, Chapter 7 proposes an alternative mechanism that shifts the focus from the location of data tied to the infrastructures to the effective jurisdiction based on intelligible access to data. The author argues that if access to intelligible personal data can be kept under control by the EEA-based data sender through, *inter alia*, strong encryption, then the actual location of the infrastructures processing such data would no longer matter. Accordingly, if appropriate technical and organisational safeguards are in place, the anticircumvention aim can be achieved without the restrictions on data exports. This is further elaborated in the concluding Chapter 8, which reiterates the importance of ensuring reasonable measures for continued compliance, rather than focusing only on data location. It is concluded that data localisation rules adopted by the EU data protection framework are not only unhelpful, but also harmful, and should therefore be abolished. If that approach sounds unrealistic in the near future, EU legislators should at least consider certain patchwork measures, including a clarification on the "transfer" concept, its underlying policy objective, the possibility of compliance by technical measures, and so on.

In terms of the structure of the book, the enquiry has been divided into the eight well-balanced chapters, each contributing a considerable amount of research to support the main argument, without any chapter feeling unnecessary or redundant. However, I wondered if it would make more sense to group Chapters 3 ("transfer" concept), 4 (legal mechanisms), and 6 (compliance and enforcement) as the first half of the main body, and Chapters 2 (legislative objectives), 5 (assumptions), and 7 (access and security approach) as the second half. This way, a reader would be given the necessary legal picture (what the law dictates and how effectively it functions) in the first place, before turning to the more critical part where the foundations of the legal framework are questioned and alternative approaches are advanced.

Having said that, the whole work remains remarkably easy to follow for the clear presentation of the sub-arguments and the compelling connections between them. Throughout the book, I find each chapter filled with insights that are sufficiently developed. As far as the substance is concerned, there are only a small number of comments here for the author to consider.

First, while it has been tightly proved that what matters is "which country or countries have effective jurisdiction over persons who control access to intelligible personal data, regardless of the data's location", (p. 321) it should be further explained what this means for the author's proposed reform of the legal framework. Does it mean that all it takes would simply be a redefinition of the scope of the restrictions (i.e. Chapter V GDPR) from "transfers of personal data to third countries" to "data processing that allows effective jurisdiction by third countries"? The author seems to suggest something more fundamental, and has even gone as far as to argue that "the [restrictions on data exports], and similar laws, should be abolished" (p. 332). Yet, just because data location does not serve as a meaningful proxy to effective jurisdiction does not mean that the mechanisms should be entirely abandoned; a counter-proposal may well be

introducing a redefinition as suggested above, thus tying the mechanisms directly to the concept of "effective jurisdiction".

This leads to a second point that the author might want to further clarify: What constitutes effective jurisdiction? As explained throughout the book, the location of the data infrastructures is neither a necessary nor sufficient condition for a third country to exercise effective jurisdiction. In practice, compelled disclosure may take many different forms, as shown in the *Microsoft warrant case* – authorities in third countries may order data controllers or processors to hand over data regardless of where they are stored, which cannot be fully addressed by technical measures such as encryption. In 2016, Facebook's Latin American Vice President was arrested for failing to comply with a court order that sought data from its subsidiary WhatsApp – which had no staff in Brazil and operated independently from Facebook, whose only office in the country only handled sales and had no access to user information.[1] Does the fact that Brazil has the power to detain a service provider's subsidiary company's local non-technical executive amount to its effective jurisdiction over the data held by that provider? If so, this concept would be subject to the same criticism made to the misplaced emphasis on data location in the case of cloud computing: "it would be complicated, impracticable, even impossible to apply the [restrictions and mechanisms] to all such locations" (p. 104).

Therefore, and coming to my third point, what EU legislators should reconsider is the role of data localisation rules in the light of their limitations. As

[1] Rob Thubron, "Facebook's Latin America VP Arrested in Brazil after Failing to Provide WhatsApp User Data" (*The Guardian*, 2 March 2016), available at https://www.techspot.com/news/63970-facebook-latin-america-vp-arrested-brazil-after-failing.html (accessed 28 December 2018). Please note that an important point is disregarded for the discussion here, one made by Facebook and WhatsApp that neither of them had access to the requested data as end-to-end encryption made it impossible.

highlighted in the book, the conflict of jurisdiction exerted by more than one country might put data controllers or processors in an extremely difficult position, which would probably require international political agreement to fully tackle (p. 333). In this regard, a more practical way forward for the GDPR – as a regional and legal framework – perhaps should not seek to avoid or even deter third countries' effective jurisdiction, but to rather focus on avoiding potential escapes from the EU's effective jurisdiction when European data subjects are involved. As observed by the author,

> [I]f the GDPR directly subjects non-EEA controllers and processors to its requirements, it should be unnecessary to restrict transfers to them *for anticircumvention reasons*. The hidden reason for retaining the Restriction in such circumstances may be concerns about the practical enforceability of EU data protection laws against such non-EEA controllers and processors. (p. 54, emphasis original)

As much as I agree that, if non-EEA data processors do not have intelligible access to the personal data (e.g. with strong encryption), the restrictions should not apply (as a "carrot" to encourage adoption of technical measures), I can equally see contractual and legal measures should be also in place in cases where it is necessary for such non-EEA entities to have access to intelligible data. Such safeguards will (at least arguably) enable data protection authorities to take enforcement actions more effectively against the controller or processor if the data are mishandled (as a "stick" to deter irresponsible sharing of data to non-EEA organisations). This will also be consistent with the author's proposition that what matters is the continued compliance with the data protection principles and accountability of data controllers, as ensuring the activities of data processors outside the EEA remain subject to the effective oversight by data protection authorities certainly forms an important part of both compliance and

accountability. Yet, as the author might agree, these measures should target who will be given intelligible access and whether they can be effectively held responsible by EEA jurisdictions, not where the data are.

To sum up, while most the book's main arguments are convincingly made, particularly regarding the mismatch between the professed policy goals and the chosen data location-centric approach in the EU data protection regime, they do not necessary lead to the conclusion that the restrictions and mechanisms are entirely unnecessary and should therefore be abandoned altogether.

Nevertheless, it should be emphasised again that *Data Localization Laws and Policy* represents a significantly well-researched and highly accessible monograph that provides important and timely observations on the EU's data localisation law and policy. Researchers, policymakers, data protection authorities and officers, and indeed anyone interested in the legal issues surrounding cross-border data flows will find the comprehensive coverage and in-depth analyses of the book significantly helpful in deciphering the complex legal and political picture.