**Asian Data Privacy Laws:
Trade and Human Rights Perspectives**

By Graham Greenleaf

Oxford: Oxford University Press, 2014. 579 pp. ISBN 9780199679669. £115.00.

When I came across Graham Greenleaf's *Asian Data Privacy Laws*, my initial thought was that this would be a useful handbook (or textbook) providing an outline of laws and perhaps some 'best practices' for addressing data privacy issues in Asia. I imagined this book being written for those who want to have an overall understanding of data privacy laws in this region – either for personal or professional interests. No sooner had I skimmed through a few pages than I realised that I my initial impression was wrong. Indeed, the breadth and depth of this book has well exceeded my expectations. It is not merely an introduction to data privacy laws in a number of Asian countries; rather, it is a critical, reflective study of data privacy regulation and research, with a global, forward-looking perspective, covering 26 jurisdictions in Asia.

Asian Data Privacy Laws is structured with three main parts. Part I sets out the foundations on which the author's observation and assessment have been conducted. One of the most important starting points of this book is that, unlike Europe, there are no regional binding treaties to protect personal data, not to mention any effective supra-national pan-Asian institutions to enforce data protection law. What makes it even more difficult to evaluate Asian data privacy laws as a whole is the notable disparities in individual countries' of approaches towards human rights, embrace of democratic ideas, legal traditions and economic development. Any attempt to start the analysis by applying an existing legal framework to these countries will therefore be doomed to fail. With this in mind, Greenleaf has instead adopted a bottom-up, inductive approach – looking into data privacy regimes with a major focus on national laws – in his search for a fair benchmark for these regimes. When it comes to such benchmark standards, it is natural to think of those that govern already mature systems like the EU's Data Protection Directive or the OECD Guidelines. Despite the relevance of these alternatives, Greenleaf has chosen an unconventional approach: applying responsive regulation theory to data privacy regulation.

First developed by Ian Ayres and John Braithwaite, responsive regulation is characterised by hierarchical pyramids with varying degrees of sanctions and incentives, from which specific measures can be chosen in response to the level of compliance. In the context of data privacy protection, this theory can been seen as a 'toolbox' filled with both carrots and sticks. Data protection enforcement is therefore considered as a construction with different sets of measures, ranging from warning letters to termination of business licences (sanctions), and from providing training to awarding compliance prizes (incentives). This theory provides a framework that can assist in assessing the organic contribution made by various mechanisms in a particular jurisdiction to the protection of personal data. This approach can thereby avoid the common pitfall of over-reliance on the analysis of only nation- or region-wide, one-size-fits-all legislations.

In Part 2, the book examines the details of specific countries, covering a total of 26 jurisdictions in 13 chapters. Some jurisdictions take up entire chapters, while others are discussed loosely in groups. The chapter on China, which is the only Asian legal system with which I am familiar,

provides a good deal of detailed and well-organised insight into the rather complicated development in this field. The term 'Warring States' is used as a metaphor in the title of this chapter to reflect the fact that there is no general data protection law, but instead sectoral or local laws in a 'patchwork, piece-by-piece form'. The complexity is exacerbated by the quasi-legislative role of China's supreme court and the uncertainty of the effect of case law. Still, Greenleaf successfully portrays a clear context by investigating statutory laws in the light of some landmark cases, with a good balance between informativeness and readability for even those unacquainted with the system. Greenleaf concludes that the advance of data privacy in China is 'complex but coherent', uncovering the potentials of China's existing laws even without comprehensive data privacy legislation. Recent developments in that country may serve to prove his observation: Article 253(a) of the Criminal Code has now been amended to unambiguously apply to all sectors;[1] the Advertising Act 2015 has reiterated the prohibition of direct marketing without individuals' consent;[2] the latest legislations concerning a wide range of subject-matters such as the tourism industry, anti-terrorism, internet maps and charities have all incorporated the requirements of protecting personal information;[3] and privacy protection has become a 'standard clause' in drafts of proposed legislation across many sectors.[4] All of these instances of an ongoing evolution could be employed to support Greenleaf's already well-evidenced remark that, despite the substantial flaws regarding principles and enforcement, 'there is increasing consistency' emerging in China.

Part III of the book moves on to draw some 'big-picture' comparative conclusions. This Part employs a considerable number of charts to carry out in-depth comparisons of the various jurisdictions with regard to their sources of privacy protection, scope of data privacy laws, data privacy principles, liabilities and cross-border implications. More importantly, by identifying distinctive regulatory models adopted across Asia, this Part investigates a highly controversial issue: is there a possible alternative to the dominant approach in the West? I would rather leave this question open and invite readers to decide for themselves after having explored this book, but it is worth mentioning here that by applying the responsive regulation theory as discussed above, Greenleaf has conducted a large-scale, evidence-supported and unprejudiced study of the functioning of a number of different options. Among all the jurisdictions covered by the book, some have transplanted the European model (e.g. Macau), while others have innovated their own theory and practice (e.g. South Korea). Some have won international acclaim for success in promoting personal data protection, while others have experienced regrettable setbacks. The absence of the need to build up a 'single market' on Asia's agenda has left this region sufficient room to experiment with different approaches, which could in turn inform the debates in the EU and other jurisdictions with well-established data privacy laws.

In the concluding chapter, Greenleaf further explores the possibility of convergence of data privacy in Asia, and in which direction, if any, it is headed. In addressing this possibility, he

---

[1] By the time of publication of this book (2014), as pointed out by the author, Article 253(a) (Infringing on citizens' personal information) applied to a list (albeit arguably an inexhaustive one) of industries. However, the latest amendment (2015) has replaced the list with a general reference to anybody, making it clear that this provision is not limited to only certain sectors.

[2] *Advertising Act 2015*, art 43. A similar provision can be found in the *Consumer Act 2013*.

[3] *Tourism Act 2013*, art 52; *Counterterrorism Act 2015*, art 48; *Regulation on Map Management 2015*, art 35; *Charity Act 2016*, art 76.

[4] For example, see draft *Public Library Act*, art 33; draft *Amendment to Insurance Act*, art 140(12); draft *Cybersecurity Act*, ch 4.

mentions the increasing importance of non-state actors. More should be said about this inspiring idea, in particular with regard to how big technology companies are engaging as privacy standard-setters in Asia. Fuelled by cloud computing and big data, the popularity of cross-border data transfers could potentially open up a forum for different data privacy laws to compete, and then eventually converge. Whether this would be for the better or for the worse is another focus of the book. Greenleaf is not as pessimistic as some theorists, who feel concerned about data privacy protection hurdling towards a 'race to the bottom'. I am inclined to share Greenleaf's confidence, believing that in the field of data protection, bad money does not necessarily drive out good. Some US-based companies, including Microsoft and Twitter, have begun to open new data centres in Europe to comply with the higher data privacy standards that exist there.[5] While it is true that businesses can relocate to countries with weaker privacy protection, the market would not. If businesses do not want to lose their customers in their target markets, they would somehow have to improve their protection to meet expectations. How regional or even global data privacy standards would thereby emerge in Europe, Asia or elsewhere in the world will be an exciting theme for upcoming research.

In sum, Greenleaf's *Asian Data Privacy Laws*, as another reviewer has pointed out, has remarkably contributed to the filling of the gap of comparative studies on national data privacy laws outside the EU.[6] Indeed, much can be learned from Asia's experience in this field, such as the development of a number of innovative data privacy principles. Yet, the problem is, on the one hand, that there is a dearth of reliable empirical materials in the English-speaking world, and, on the other hand, that there is arguably a fetishism of the European model in both parts of the world. Thus, the most significant contribution of this book is that it offers a novel and sound paradigm for the evaluation of a particular country's data protection system, one that is not confined to the stereotype that a good data privacy regime must be all-sector, principle-driven and human rights-oriented. From that point of view, *Asian Data Privacy Laws* is not just intended for those who are interested in Asian countries; it is also relevant to all data protection researchers, practitioners, regulators and policymakers. It illustrates a vivid data privacy landscape that is radically different from that of the West, and, more crucially, it provides a wider horizon of data privacy regulation with certain unexplored possibilities.

Jiahong Chen
PhD Candidate, School of Law, University of Edinburgh

---

[5] The Guardian, "Microsoft to open first UK data centres" (2015) available at http://www.theguardian.com/technology/2015/nov/10/microsoft-open-first-uk-data-centres-safe-harbour (accessed 28 Mar 16); Financial Times, "Microsoft unveils German data plan to tackle US internet spying" (2015) available at http://www.ft.com/cms/s/0/540a296e-87ff-11e5-9f8c-a8d619fa707c.html (accessed 28 Mar 16); M Bennett, "NetSuite: European data centre is not needed for privacy or compliance" (2015) available at http://www.v3.co.uk/v3-uk/analysis/2407322/netsuite-european-data-centre-is-not-needed-for-privacy-or-compliance (accessed 28 Mar 16).
[6] D Vaile, "Data Privacy Law in the Asian Region: Review of 'Asian Data Privacy Laws – Trade and Human Rights Perspectives' by Graham Greenleaf" (2015) 3 *Australian Journal of Telecommunications and the Digital Economy* 60-63, at 60.